IE340 Series

INDUSTRIAL ETHERNET LAYER 3 SWITCHES

IE340-12GP **IE340-20GP**
IE340-12GT **IE340L-18GP**

Command Reference for AlliedWare Plus™ Version 5.5.1-0.x

C613-50463-01 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 ©1998-2008 The OpenSSL Project. All rights reserved.

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

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

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.

© 2021 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 111

Chapter 1: CLI Navigation Commands 112

Introduction 112
configure terminal 113
disable (Privileged Exec mode) 114
do 115
enable (Privileged Exec mode) 116
end 118
exit 119
help 120
logout 121
show history 122

Chapter 2: Device GUI and Vista Manager EX Commands 123

Introduction 123
atmf topology-gui enable 124
http log webapi-requests 125
http port 126
http secure-port 127
log event-host 128
service http 129
show http 130

Chapter 3: File and Configuration Management Commands 131

Introduction 131
autoboot enable 134
boot config-file 135
boot config-file backup 137
boot system 138
boot system backup 139
cd 140
copy (filename) 141

copy debug 143
copy running-config 144
copy startup-config 145
copy zmodem 146
create autoboot 147
crypto verify 148
delete 150
delete debug 151
dir 152
edit 154
edit (filename) 155
erase factory-default 156
erase startup-config 157
ip tftp source-interface 158
ipv6 tftp source-interface 159
mkdir 160
move 161
move debug 162
pwd 163
rmdir 164
show autoboot 165
show boot 166
show file 168
show file systems 169
show running-config 171
show running-config interface 174
show startup-config 177
show version 178
unmount 179
write file 180
write memory 181
write terminal 182

Chapter 4: User Access Commands 183

Introduction 183
aaa authentication enable default local 185
aaa local authentication attempts lockout-time 186
aaa local authentication attempts max-fail 187
aaa login fail-delay 188
clear aaa local user lockout 189
clear line console 190
clear line vty 191
enable password 192
enable secret (deprecated) 195
exec-timeout 196
flowcontrol hardware (asyn/console) 198
length (asyn) 200
line 201
privilege level 203
security-password history 204
security-password forced-change 205
security-password lifetime 206
security-password min-lifetime-enforce 207

security-password minimum-categories 208
security-password minimum-length 209
security-password reject-expired-pwd 210
security-password warning 211
service advanced-vty 212
service password-encryption 213
service telnet 214
show aaa local user locked 215
show privilege 216
show security-password configuration 217
show security-password user 218
show telnet 219
show users 220
telnet 221
telnet server 222
terminal length 223
terminal resize 224
username 225

Chapter 5: Feature Licensing Commands 227
Introduction 227
license 228
show license 230
show license brief 232

Chapter 6: Subscription Licensing Commands 234
Introduction 234
license update file 235
license update online 236
show license external 237

Chapter 7: System Configuration and Monitoring Commands 238
Introduction 238
banner exec 240
banner login (system) 242
banner motd 244
clock set 246
clock summer-time date 247
clock summer-time recurring 249
clock timezone 251
continuous-reboot-prevention 252
crypto secure-mode 254
debug core-file 255
ecofriendly led 256
ecofriendly lpi 257
findme 259
findme trigger 261
hostname 262
max-fib-routes 264
max-static-routes 265
no debug all 266
reboot 268

reload 269
show clock 270
show continuous-reboot-prevention 272
show cpu 273
show cpu history 276
show debugging 278
show ecofriendly 279
show interface memory 281
show memory 283
show memory allocations 285
show memory history 287
show memory pools 288
show memory shared 289
show process 290
show reboot history 292
show router-id 293
show secure-mode 294
show system 295
show system environment 296
show system environment counters 297
show system interrupts 299
show system mac 300
show system pci device 301
show system pci tree 302
show system serialnumber 303
show tech-support 304
speed (asyn) 306
terminal monitor 308
undebug all 309

Chapter 8: Pluggables and Cabling Commands 310

Introduction 310
clear fiber-monitoring interface 311
clear test cable-diagnostics tdr 312
debug fiber-monitoring 313
fiber-monitoring action 315
fiber-monitoring baseline 317
fiber-monitoring enable 319
fiber-monitoring interval 320
fiber-monitoring sensitivity 321
show system fiber-monitoring 323
show system pluggable 326
show system pluggable detail 328
show system pluggable diagnostics 331
show test cable-diagnostics tdr 333
test cable-diagnostics tdr interface 334

Chapter 9: Connectivity Fault Management Commands 335

Introduction 335
cc interval 337
cc multicast 339
cc unicast 340

clear (MEP Attribute) 341
clear ethernet cfm errorlog 342
clear mep counter 343
ethernet cfm domain-name 344
ethernet cfm mep 347
mep (FNG attributes) 349
mep active 351
mep ccm-ltm-priority 353
mep crosscheck 355
service ma-name 357
show ethernet cfm details 360
show ethernet cfm domain 365
show ethernet cfm errorlog 368
show ethernet cfm maintenance-points local mep 370
show ethernet cfm maintenance-points remote mep 376
show ethernet cfm service 379
show mep-alarm status 382

Chapter 10: Logging Commands 383
Introduction 383
clear exception log 385
clear log 386
clear log buffered 387
clear log external 388
clear log permanent 389
copy buffered-log 390
copy permanent-log 391
default log buffered 392
default log console 393
default log email 394
default log external 395
default log host 396
default log monitor 397
default log permanent 398
log buffered 399
log buffered (filter) 400
log buffered exclude 403
log buffered size 406
log console 407
log console (filter) 408
log console exclude 411
log email 414
log email (filter) 415
log email exclude 418
log email time 421
log external 423
log external (filter) 425
log external exclude 428
log external rotate 431
log external size 433
log facility 434
log host 436
log host (filter) 438

log host exclude 441
log host source 444
log host startup-delay 445
log host time 447
log monitor (filter) 449
log monitor exclude 452
log permanent 455
log permanent (filter) 456
log permanent exclude 459
log permanent size 462
log-rate-limit nsm 463
log trustpoint 464
show counter log 465
show exception log 466
show log 467
show log config 469
show log external 471
show log permanent 472
show running-config log 473
unmount 474

Chapter 11: Scripting Commands 475
Introduction 475
activate 476
echo 477
wait 478

Chapter 12: Interface Commands 479
Introduction 479
description (interface) 480
interface (to configure) 481
mru 483
mtu 484
service statistics interfaces counter 485
show interface 486
show interface brief 489
show interface memory 490
show interface status 492
shutdown 494

Chapter 13: Port Mirroring and Remote Mirroring Commands 495
Introduction 495
mirror interface 496
remote-mirror interface 498
show mirror 500
show mirror interface 501
show remote-mirror 502
switchport remote-mirror-egress 504
vlan mode remote-mirror-vlan 505

Chapter 14: Alarm Monitoring Commands 507
Introduction 507

alarm facility epsr led 509
alarm facility epsr relay 510
alarm facility g8032 led 511
alarm facility g8032 relay 512
alarm facility input-alarm alarm-position 513
alarm facility input-alarm led 514
alarm facility input-alarm relay 516
alarm facility link-down led 518
alarm facility link-down relay 519
alarm facility loopprot led 520
alarm facility loopprot relay 521
alarm facility main-pse led 522
alarm facility main-pse relay 523
alarm facility power-supply led 524
alarm facility power-supply relay 525
alarm facility pse-port led 526
alarm facility pse-port relay 527
alarm facility temperature led 529
alarm facility temperature relay 530
alarm facility ufo led 531
alarm facility ufo relay 532
debug alarm 533
show alarm facility settings 534
show alarm facility status 535
show debugging alarm 536

PART 2: Interfaces and Layer 2 537

Chapter 15: Switching Commands 538
Introduction 538
backpressure 540
clear loop-protection action 542
clear loop-protection counters 543
clear mac address-table dynamic 544
clear mac address-table static 546
clear port counter 547
clear port-security intrusion 548
cut-through 550
debug loopprot 551
debug platform packet 552
duplex 554
flowcontrol (switch port) 555
linkflap action 557
loop-protection loop-detect 558
loop-protection action 559
loop-protection action-delay-time 560
loop-protection timeout 561
mac address-table acquire 562
mac address-table ageing-time 563
mac address-table logging 564
mac address-table static 565
mac address-table thrash-limit 566

platform hwfilter-size . . . 567
platform l3-vlan-hashing-algorithm . . . 568
platform load-balancing . . . 569
platform mac-vlan-hashing-algorithm . . . 570
platform multicast-ratelimit . . . 571
platform stop-unreg-mc-flooding . . . 572
platform vlan-stacking-tpid . . . 574
polarity . . . 575
show debugging loopprot . . . 576
show debugging platform packet . . . 577
show flowcontrol interface . . . 578
show interface err-disabled . . . 579
show interface switchport . . . 580
show loop-protection . . . 581
show mac address-table . . . 583
show mac address-table thrash-limit . . . 585
show platform . . . 586
show platform classifier statistics utilization brief . . . 589
show platform port . . . 591
show port-security interface . . . 593
show port-security intrusion . . . 594
show storm-control . . . 595
speed . . . 596
storm-control level . . . 598
switchport port-security . . . 599
switchport port-security aging . . . 601
switchport port-security maximum . . . 603
switchport port-security violation . . . 605
thrash-limiting . . . 607
undebug loopprot . . . 609
undebug platform packet . . . 610

Chapter 16: VLAN Commands . . . 611
Introduction . . . 611
debug private-vlan ufo . . . 613
platform vlan-stacking-tpid . . . 614
port-vlan-forwarding-priority . . . 615
private-vlan . . . 618
private-vlan association . . . 620
private-vlan ufo trap . . . 621
show debugging private-vlan . . . 622
show interface switchport vlan translation . . . 623
show port-vlan-forwarding-priority . . . 625
show vlan . . . 626
show vlan access-map . . . 627
show vlan classifier group . . . 628
show vlan classifier group interface . . . 629
show vlan classifier interface group . . . 630
show vlan classifier rule . . . 631
show vlan filter . . . 632
show vlan private-vlan . . . 633
show vlan private-vlan ufo . . . 634
switchport access vlan . . . 635

switchport enable vlan 636
switchport mode access 637
switchport mode private-vlan 638
switchport mode private-vlan trunk promiscuous 639
switchport mode private-vlan trunk secondary 641
switchport mode private-vlan ufo 643
switchport mode trunk 645
switchport private-vlan host-association 646
switchport private-vlan mapping 647
switchport trunk allowed vlan 648
switchport trunk native vlan 651
switchport vlan translation 652
switchport vlan translation default drop 654
switchport vlan-stacking (double-tagging) 655
switchport voice dscp 656
switchport voice vlan 657
switchport voice vlan priority 659
vlan 660
vlan access-map 662
vlan classifier activate 663
vlan classifier group 664
vlan classifier rule ipv4 665
vlan classifier rule proto 666
vlan database 669
vlan filter 670

Chapter 17: Spanning Tree Commands 671

Introduction 671
clear spanning-tree statistics 673
clear spanning-tree detected protocols (RSTP and MSTP) 674
debug mstp (RSTP and STP) 675
instance priority (MSTP) 679
instance vlan (MSTP) 681
region (MSTP) 683
revision (MSTP) 684
show debugging mstp 685
show spanning-tree 686
show spanning-tree brief 689
show spanning-tree mst 690
show spanning-tree mst config 691
show spanning-tree mst detail 692
show spanning-tree mst detail interface 694
show spanning-tree mst instance 696
show spanning-tree mst instance interface 697
show spanning-tree mst interface 698
show spanning-tree statistics 699
show spanning-tree statistics instance 701
show spanning-tree statistics instance interface 702
show spanning-tree statistics interface 704
show spanning-tree vlan range-index 706
spanning-tree autoedge (RSTP and MSTP) 707
spanning-tree bpdu 708
spanning-tree cisco-interoperability (MSTP) 710

spanning-tree edgeport (RSTP and MSTP) 711
spanning-tree enable 712
spanning-tree errdisable-timeout enable 714
spanning-tree errdisable-timeout interval 715
spanning-tree force-version 716
spanning-tree forward-time 717
spanning-tree guard root 718
spanning-tree hello-time 719
spanning-tree link-type 720
spanning-tree max-age 721
spanning-tree max-hops (MSTP) 722
spanning-tree mode 723
spanning-tree mst configuration 724
spanning-tree mst instance 725
spanning-tree mst instance path-cost 726
spanning-tree mst instance priority 728
spanning-tree mst instance restricted-role 729
spanning-tree mst instance restricted-tcn 731
spanning-tree path-cost 732
spanning-tree portfast (STP) 733
spanning-tree portfast bpdu-filter 735
spanning-tree portfast bpdu-guard 737
spanning-tree priority (bridge priority) 739
spanning-tree priority (port priority) 740
spanning-tree restricted-role 741
spanning-tree restricted-tcn 742
spanning-tree transmit-holdcount 743
undebug mstp 744

Chapter 18: Unidirectional Link Detection (UDLD) Commands 745
Introduction 745
debug udld 746
show debugging udld 747
show udld 748
show udld neighbors 749
show udld port 750
udld aggressive-mode 751
udld enable 752
udld port 753
udld port aggressive-mode 754
udld port disable 755
udld reset 756
udld time disable-period 757
udld time message-interval 758
undebug udld 759

Chapter 19: Link Aggregation Commands 760
Introduction 760
channel-group 762
clear lacp counters 764
debug lacp 765
lacp global-passive-mode enable 766

lacp port-priority 767
lacp system-priority 768
lacp timeout 769
platform load-balancing 771
show debugging lacp 772
show diagnostic channel-group 773
show etherchannel 775
show etherchannel detail 776
show etherchannel summary 777
show lacp sys-id 778
show lacp-counter 779
show port etherchannel 780
show static-channel-group 781
static-channel-group 782
undebug lacp 784

Chapter 20: Power over Ethernet Commands 785
Introduction 785
clear power-inline counters interface 787
debug power-inline 788
power-inline allow-legacy 790
power-inline description 791
power-inline enable 792
power-inline hanp 793
power-inline max 794
power-inline priority 796
power-inline usage-threshold 798
power-inline wattage max 799
service power-inline 800
show debugging power-inline 801
show power-inline 802
show power-inline counters 806
show power-inline interface 808
show power-inline interface detail 811

Chapter 21: GVRP Commands 814
Introduction 814
clear gvrp statistics 815
debug gvrp 816
gvrp (interface) 818
gvrp dynamic-vlan-creation 819
gvrp enable (global) 820
gvrp registration 821
gvrp timer 822
show debugging gvrp 824
show gvrp configuration 825
show gvrp machine 826
show gvrp statistics 827
show gvrp timer 828

PART 3: Layer 3 Switching 829

Chapter 22: IP Addressing and Protocol Commands 830
Introduction 830
arp-aging-timeout 832
arp-mac-disparity 833
arp 836
arp log 838
arp opportunistic-nd 841
arp-reply-bc-dmac 842
clear arp-cache 843
debug ip packet interface 844
debug ip irdp 846
ip address (IP Addressing and Protocol) 847
ip directed-broadcast 849
ip forwarding 851
ip forward-protocol udp 852
ip gratuitous-arp-link 854
ip helper-address 856
ip irdp 858
ip icmp error-interval 859
ip irdp address preference 860
ip irdp broadcast 861
ip irdp holdtime 862
ip irdp lifetime 863
ip irdp maxadvertinterval 864
ip irdp minadvertinterval 866
ip irdp multicast 868
ip irdp preference 869
ip limited-local-proxy-arp 870
ip local-proxy-arp 871
ip proxy-arp 872
ip redirects 873
ip tcp synack-retries 874
ip unreachables 875
local-proxy-arp 877
optimistic-nd 878
ping 879
router ip irdp 880
show arp 881
show debugging ip packet 882
show ip flooding-nexthops 883
show ip forwarding 884
show ip interface 885
show ip irdp 886
show ip irdp interface 887
show ip sockets 889
show ip traffic 892
tcpdump 894
traceroute 895
undebug ip packet interface 896
undebug ip irdp 897

Chapter 23: Domain Name Service (DNS) Commands 898

Introduction 898
clear ip dns forwarding cache 900
debug ip dns forwarding 901
ip dns forwarding 902
ip dns forwarding cache 903
ip dns forwarding dead-time 904
ip dns forwarding retry 905
ip dns forwarding source-interface 906
ip dns forwarding timeout 907
ip domain-list 908
ip domain-lookup 909
ip domain-name 911
ip name-server 912
ip name-server preferred-order 914
show debugging ip dns forwarding 915
show hosts 916
show ip dns forwarding 917
show ip dns forwarding cache 918
show ip dns forwarding server 919
show ip domain-list 920
show ip domain-name 921
show ip name-server 922

Chapter 24: IPv6 Commands 923

Introduction 923
clear ipv6 neighbors 925
ipv6 address 926
ipv6 address autoconfig 928
ipv6 address suffix 930
ipv6 enable 931
ipv6 eui64-linklocal 933
ipv6 forwarding 934
ipv6 icmp error-interval 935
ipv6 multicast forward-slow-path-packet 936
ipv6 nd accept-ra-default-routes 937
ipv6 nd accept-ra-pinfo 938
ipv6 nd current-hoplimit 939
ipv6 nd dns search-list 940
ipv6 nd dns-server 941
ipv6 nd managed-config-flag 942
ipv6 nd minimum-ra-interval 943
ipv6 nd other-config-flag 944
ipv6 nd prefix 945
ipv6 nd ra-interval 947
ipv6 nd ra-lifetime 948
ipv6 nd raguard 949
ipv6 nd reachable-time 951
ipv6 nd retransmission-time 952
ipv6 nd route-information 953
ipv6 nd router-preference 954
ipv6 nd suppress-ra 955
ipv6 neighbor 956
ipv6 opportunistic-nd 957

ipv6 route 958
ipv6 unreachables 959
optimistic-nd 960
ping ipv6 961
show ipv6 forwarding 963
show ipv6 interface 964
show ipv6 neighbors 965
show ipv6 route 966
show ipv6 route summary 968
traceroute ipv6 969

Chapter 25: Routing Commands 970
Introduction 970
ip route 971
ipv6 route 973
max-fib-routes 974
max-static-routes 975
maximum-paths 976
show ip route 977
show ip route database 980
show ip route summary 982
show ipv6 route 983
show ipv6 route summary 985

Chapter 26: RIP Commands 986
Introduction 986
accept-lifetime 988
alliedware-behavior 990
cisco-metric-behavior (RIP) 992
clear ip rip route 993
debug rip 994
default-information originate (RIP) 995
default-metric (RIP) 996
distance (RIP) 997
distribute-list (RIP) 998
fullupdate (RIP) 999
ip summary-address rip 1000
ip prefix-list 1001
ip rip authentication key-chain 1003
ip rip authentication mode 1005
ip rip authentication string 1008
ip rip receive-packet 1010
ip rip receive version 1011
ip rip send-packet 1012
ip rip send version 1013
ip rip send version 1-compatible 1015
ip rip split-horizon 1017
key 1018
key chain 1019
key-string 1020
maximum-prefix 1021
neighbor (RIP) 1022

network (RIP) . . . 1023
offset-list (RIP) . . . 1024
passive-interface (RIP) . . . 1025
recv-buffer-size (RIP) . . . 1026
redistribute (RIP) . . . 1027
restart rip graceful . . . 1028
rip restart grace-period . . . 1029
route (RIP) . . . 1030
router rip . . . 1031
send-lifetime . . . 1032
show debugging rip . . . 1034
show ip prefix-list . . . 1035
show ip protocols rip . . . 1036
show ip rip . . . 1037
show ip rip database . . . 1038
show ip rip interface . . . 1039
timers (RIP) . . . 1040
undebug rip . . . 1041
version (RIP) . . . 1042

Chapter 27: RIPng for IPv6 Commands . . . 1043
Introduction . . . 1043
aggregate-address (IPv6 RIPng) . . . 1045
clear ipv6 rip route . . . 1046
debug ipv6 rip . . . 1047
default-information originate (IPv6 RIPng) . . . 1048
default-metric (IPv6 RIPng) . . . 1049
distribute-list (IPv6 RIPng) . . . 1050
ipv6 prefix-list . . . 1051
ipv6 rip metric-offset . . . 1053
ipv6 rip split-horizon . . . 1055
ipv6 router rip . . . 1056
neighbor (IPv6 RIPng) . . . 1057
offset-list (IPv6 RIPng) . . . 1058
passive-interface (IPv6 RIPng) . . . 1059
recv-buffer-size (IPv6 RIPng) . . . 1060
redistribute (IPv6 RIPng) . . . 1061
route (IPv6 RIPng) . . . 1062
router ipv6 rip . . . 1063
show debugging ipv6 rip . . . 1064
show ipv6 prefix-list . . . 1065
show ipv6 protocols rip . . . 1066
show ipv6 rip . . . 1067
show ipv6 rip database . . . 1068
show ipv6 rip interface . . . 1069
timers (IPv6 RIPng) . . . 1070
undebug ipv6 rip . . . 1071

Chapter 28: OSPF Commands . . . 1072
Introduction . . . 1072
area default-cost . . . 1075
area authentication . . . 1076

area filter-list . . . 1077
area nssa . . . 1078
area range . . . 1080
area stub . . . 1082
area virtual-link . . . 1083
auto-cost reference bandwidth . . . 1086
bandwidth . . . 1088
capability opaque . . . 1089
capability restart . . . 1090
clear ip ospf process . . . 1091
compatible rfc1583 . . . 1092
debug ospf events . . . 1093
debug ospf ifsm . . . 1094
debug ospf lsa . . . 1095
debug ospf nfsm . . . 1096
debug ospf nsm . . . 1097
debug ospf packet . . . 1098
debug ospf route . . . 1099
default-information originate . . . 1100
default-metric (OSPF) . . . 1101
distance (OSPF) . . . 1102
distribute-list (OSPF) . . . 1104
enable db-summary-opt . . . 1107
host area . . . 1108
ip ospf authentication . . . 1109
ip ospf authentication-key . . . 1110
ip ospf cost . . . 1111
ip ospf database-filter . . . 1112
ip ospf dead-interval . . . 1113
ip ospf disable all . . . 1114
ip ospf hello-interval . . . 1115
ip ospf message-digest-key . . . 1116
ip ospf mtu . . . 1118
ip ospf mtu-ignore . . . 1119
ip ospf network . . . 1120
ip ospf priority . . . 1121
ip ospf resync-timeout . . . 1122
ip ospf retransmit-interval . . . 1123
ip ospf transmit-delay . . . 1124
max-concurrent-dd . . . 1125
maximum-area . . . 1126
neighbor (OSPF) . . . 1127
network area . . . 1128
ospf abr-type . . . 1130
ospf restart grace-period . . . 1131
ospf restart helper . . . 1132
ospf router-id . . . 1134
overflow database . . . 1135
overflow database external . . . 1136
passive-interface (OSPF) . . . 1137
redistribute (OSPF) . . . 1138
restart ospf graceful . . . 1140
router ospf . . . 1141

router-id 1142
show debugging ospf 1143
show ip ospf 1144
show ip ospf border-routers 1147
show ip ospf database 1148
show ip ospf database asbr-summary 1150
show ip ospf database external 1151
show ip ospf database network 1153
show ip ospf database nssa-external 1154
show ip ospf database opaque-area 1156
show ip ospf database opaque-as 1157
show ip ospf database opaque-link 1158
show ip ospf database router 1159
show ip ospf database summary 1161
show ip ospf interface 1164
show ip ospf neighbor 1165
show ip ospf route 1167
show ip ospf virtual-links 1168
show ip protocols ospf 1169
summary-address 1170
timers spf exp 1171
undebug ospf events 1172
undebug ospf ifsm 1173
undebug ospf lsa 1174
undebug ospf nfsm 1175
undebug ospf nsm 1176
undebug ospf packet 1177
undebug ospf route 1178

Chapter 29: OSPFv3 for IPv6 Commands 1179

Introduction 1179
abr-type 1182
area authentication ipsec spi 1183
area default-cost (IPv6 OSPF) 1185
area encryption ipsec spi esp 1186
area range (IPv6 OSPF) 1189
area stub (IPv6 OSPF) 1191
area virtual-link (IPv6 OSPF) 1192
area virtual-link authentication ipsec spi 1194
area virtual-link encryption ipsec spi 1196
auto-cost reference bandwidth (IPv6 OSPF) 1199
bandwidth 1201
clear ipv6 ospf process 1202
debug ipv6 ospf events 1203
debug ipv6 ospf ifsm 1204
debug ipv6 ospf lsa 1205
debug ipv6 ospf nfsm 1206
debug ipv6 ospf packet 1207
debug ipv6 ospf route 1208
default-information originate 1209
default-metric (IPv6 OSPF) 1210
distance (IPv6 OSPF) 1211
distribute-list (IPv6 OSPF) 1213

ipv6 ospf authentication spi 1215
ipv6 ospf cost 1217
ipv6 ospf dead-interval 1218
ipv6 ospf display route single-line 1219
ipv6 ospf encryption spi esp 1220
ipv6 ospf hello-interval 1223
ipv6 ospf neighbor 1224
ipv6 ospf network 1226
ipv6 ospf priority 1227
ipv6 ospf retransmit-interval 1228
ipv6 ospf transmit-delay 1229
ipv6 router ospf area 1230
max-concurrent-dd (IPv6 OSPF) 1232
passive-interface (IPv6 OSPF) 1233
redistribute (IPv6 OSPF) 1234
restart ipv6 ospf graceful 1236
router ipv6 ospf 1237
router-id (IPv6 OSPF) 1238
show debugging ipv6 ospf 1239
show ipv6 ospf 1240
show ipv6 ospf database 1242
show ipv6 ospf database external 1244
show ipv6 ospf database grace 1245
show ipv6 ospf database inter-prefix 1246
show ipv6 ospf database inter-router 1247
show ipv6 ospf database intra-prefix 1248
show ipv6 ospf database link 1249
show ipv6 ospf database network 1250
show ipv6 ospf database router 1252
show ipv6 ospf interface 1257
show ipv6 ospf neighbor 1259
show ipv6 ospf route 1261
show ipv6 ospf virtual-links 1263
summary-address (IPv6 OSPF) 1264
timers spf exp (IPv6 OSPF) 1266
undebug ipv6 ospf events 1267
undebug ipv6 ospf ifsm 1268
undebug ipv6 ospf lsa 1269
undebug ipv6 ospf nfsm 1270
undebug ipv6 ospf packet 1271
undebug ipv6 ospf route 1272

Chapter 30: BGP and BGP4+ Commands 1273

Introduction 1273
address-family 1279
aggregate-address 1281
auto-summary (BGP only) 1284
bgp aggregate-nexthop-check 1286
bgp always-compare-med 1287
bgp bestpath as-path ignore 1289
bgp bestpath compare-confed-aspath 1290
bgp bestpath compare-routerid 1291
bgp bestpath med 1292

bgp bestpath med remove-recv-med 1294
bgp bestpath med remove-send-med 1295
bgp client-to-client reflection 1296
bgp cluster-id 1297
bgp confederation identifier 1299
bgp confederation peers 1300
bgp config-type 1302
bgp dampening 1304
bgp damp-peer-oscillation (BGP only) 1306
bgp default ipv4-unicast 1307
bgp default local-preference (BGP only) 1308
bgp deterministic-med 1309
bgp enforce-first-as 1311
bgp fast-external-failover 1312
bgp graceful-restart 1313
bgp graceful-restart graceful-reset 1315
bgp log-neighbor-changes 1316
bgp memory maxallocation 1318
bgp nexthop-trigger-count 1319
bgp nexthop-trigger delay 1320
bgp nexthop-trigger enable 1321
bgp rfc1771-path-select (BGP only) 1322
bgp rfc1771-strict (BGP only) 1323
bgp router-id 1324
bgp scan-time (BGP only) 1326
bgp update-delay 1327
clear bgp * 1328
clear bgp (IPv4 or IPv6 address) 1329
clear bgp (ASN) 1331
clear bgp external 1332
clear bgp peer-group 1333
clear bgp ipv6 (ipv6 address) (BGP4+ only) 1334
clear bgp ipv6 dampening (BGP4+ only) 1335
clear bgp ipv6 flap-statistics (BGP4+ only) 1336
clear bgp ipv6 (ASN) (BGP4+ only) 1337
clear bgp ipv6 external (BGP4+ only) 1338
clear bgp ipv6 peer-group (BGP4+ only) 1339
clear ip bgp * (BGP only) 1340
clear ip bgp (IPv4) (BGP only) 1341
clear ip bgp dampening (BGP only) 1342
clear ip bgp flap-statistics (BGP only) 1343
clear ip bgp (ASN) (BGP only) 1344
clear ip bgp external (BGP only) 1345
clear ip bgp peer-group (BGP only) 1346
clear ip prefix-list 1347
debug bgp (BGP only) 1348
distance (BGP and BGP4+) 1350
exit-address-family 1352
ip as-path access-list 1353
ip community-list 1355
ip community-list expanded 1357
ip community-list standard 1359
ip extcommunity-list expanded 1361

ip extcommunity-list standard 1363
ip prefix-list 1365
ipv6 prefix-list 1367
match as-path 1369
match community 1371
max-paths 1373
neighbor activate 1374
neighbor advertisement-interval 1377
neighbor allowas-in 1380
neighbor as-origination-interval 1383
neighbor attribute-unchanged 1385
neighbor capability graceful-restart 1388
neighbor capability orf prefix-list 1391
neighbor capability route-refresh 1394
neighbor collide-established 1397
neighbor default-originate 1400
neighbor description 1403
neighbor disallow-infinite-holdtime 1406
neighbor distribute-list 1408
neighbor dont-capability-negotiate 1411
neighbor ebgp-multihop 1414
neighbor enforce-multihop 1417
neighbor filter-list 1420
neighbor interface 1423
neighbor local-as 1424
neighbor maximum-prefix 1427
neighbor next-hop-self 1430
neighbor override-capability 1433
neighbor passive 1435
neighbor password 1438
neighbor peer-group (add a neighbor) 1441
neighbor peer-group (create a peer-group) 1443
neighbor port 1444
neighbor prefix-list 1447
neighbor remote-as 1450
neighbor remove-private-AS (BGP only) 1453
neighbor restart-time 1455
neighbor route-map 1458
neighbor route-reflector-client (BGP only) 1462
neighbor route-server-client (BGP only) 1464
neighbor send-community 1465
neighbor shutdown 1469
neighbor soft-reconfiguration inbound 1471
neighbor timers 1474
neighbor transparent-as 1477
neighbor transparent-nexthop 1479
neighbor unsuppress-map 1481
neighbor update-source 1484
neighbor version (BGP only) 1488
neighbor weight 1490
network (BGP and BGP4+) 1493
network synchronization 1496
redistribute (into BGP or BGP4+) 1497

restart bgp graceful (BGP only) 1499
router bgp 1500
route-map 1501
set as-path 1504
set community 1505
show bgp ipv6 (BGP4+ only) 1507
show bgp ipv6 community (BGP4+ only) 1508
show bgp ipv6 community-list (BGP4+ only) 1510
show bgp ipv6 dampening (BGP4+ only) 1511
show bgp ipv6 filter-list (BGP4+ only) 1512
show bgp ipv6 inconsistent-as (BGP4+ only) 1513
show bgp ipv6 longer-prefixes (BGP4+ only) 1514
show bgp ipv6 neighbors (BGP4+ only) 1515
show bgp ipv6 paths (BGP4+ only) 1518
show bgp ipv6 prefix-list (BGP4+ only) 1519
show bgp ipv6 quote-regexp (BGP4+ only) 1520
show bgp ipv6 regexp (BGP4+ only) 1521
show bgp ipv6 route-map (BGP4+ only) 1523
show bgp ipv6 summary (BGP4+ only) 1524
show bgp memory maxallocation (BGP only) 1525
show bgp nexthop-tracking (BGP only) 1526
show bgp nexthop-tree-details (BGP only) 1527
show debugging bgp (BGP only) 1528
show ip bgp (BGP only) 1529
show ip bgp attribute-info (BGP only) 1530
show ip bgp cidr-only (BGP only) 1531
show ip bgp community (BGP only) 1532
show ip bgp community-info (BGP only) 1534
show ip bgp community-list (BGP only) 1535
show ip bgp dampening (BGP only) 1536
show ip bgp filter-list (BGP only) 1538
show ip bgp inconsistent-as (BGP only) 1539
show ip bgp longer-prefixes (BGP only) 1540
show ip bgp neighbors (BGP only) 1541
show ip bgp neighbors connection-retrytime (BGP only) 1544
show ip bgp neighbors hold-time (BGP only) 1545
show ip bgp neighbors keepalive (BGP only) 1546
show ip bgp neighbors keepalive-interval (BGP only) 1547
show ip bgp neighbors notification (BGP only) 1548
show ip bgp neighbors open (BGP only) 1549
show ip bgp neighbors rcvd-msgs (BGP only) 1550
show ip bgp neighbors sent-msgs (BGP only) 1551
show ip bgp neighbors update (BGP only) 1552
show ip bgp paths (BGP only) 1553
show ip bgp prefix-list (BGP only) 1554
show ip bgp quote-regexp (BGP only) 1555
show ip bgp regexp (BGP only) 1557
show ip bgp route-map (BGP only) 1559
show ip bgp scan (BGP only) 1560
show ip bgp summary (BGP only) 1561
show ip community-list 1562
show ip extcommunity-list 1563
show ip prefix-list 1564

show ipv6 prefix-list . . . 1565
show ip protocols bgp (BGP only) . . . 1566
show route-map . . . 1567
synchronization . . . 1568
timers (BGP) . . . 1570
undebug bgp (BGP only) . . . 1572

Chapter 31: Route Map Commands . . . 1573
Introduction . . . 1573
match as-path . . . 1575
match community . . . 1577
match interface . . . 1579
match ip address . . . 1580
match ip next-hop . . . 1582
match ipv6 address . . . 1584
match ipv6 next-hop . . . 1586
match metric . . . 1587
match origin . . . 1588
match route-type . . . 1590
match tag . . . 1591
route-map . . . 1592
set aggregator . . . 1595
set as-path . . . 1596
set atomic-aggregate . . . 1597
set comm-list delete . . . 1598
set community . . . 1599
set dampening . . . 1601
set extcommunity . . . 1603
set ip next-hop (route map) . . . 1605
set ipv6 next-hop . . . 1606
set local-preference . . . 1607
set metric . . . 1608
set metric-type . . . 1610
set origin . . . 1611
set originator-id . . . 1612
set tag . . . 1613
set weight . . . 1614
show route-map . . . 1615

PART 4: Multicast Applications . . . 1616

Chapter 32: IGMP and IGMP Snooping Commands . . . 1617
Introduction . . . 1617
clear ip igmp . . . 1619
clear ip igmp group . . . 1620
clear ip igmp interface . . . 1621
debug igmp . . . 1622
ip igmp . . . 1623
ip igmp access-group . . . 1624
ip igmp flood-group . . . 1625
ip igmp flood specific-query . . . 1627
ip igmp immediate-leave . . . 1628

ip igmp last-member-query-count 1629
ip igmp last-member-query-interval 1630
ip igmp limit 1631
ip igmp maximum-groups 1632
ip igmp mroute-proxy 1634
ip igmp proxy-service 1635
ip igmp querier-timeout 1636
ip igmp query-holdtime 1637
ip igmp query-interval 1639
ip igmp query-max-response-time 1641
ip igmp ra-option 1643
ip igmp robustness-variable 1644
ip igmp snooping 1645
ip igmp snooping fast-leave 1646
ip igmp snooping mrouter 1647
ip igmp snooping querier 1648
ip igmp snooping report-suppression 1649
ip igmp snooping routermode 1650
ip igmp snooping source-timeout 1652
ip igmp snooping tcn query solicit 1653
ip igmp source-address-check 1655
ip igmp ssm 1656
ip igmp ssm-map enable 1657
ip igmp ssm-map static 1658
ip igmp static-group 1660
ip igmp startup-query-count 1662
ip igmp startup-query-interval 1663
ip igmp trusted 1664
ip igmp version 1665
show debugging igmp 1666
show ip igmp groups 1667
show ip igmp interface 1669
show ip igmp proxy 1671
show ip igmp proxy groups 1672
show ip igmp snooping mrouter 1674
show ip igmp snooping routermode 1675
show ip igmp snooping source-timeout 1676
show ip igmp snooping statistics 1677
undebug igmp 1679

Chapter 33: MLD and MLD Snooping Commands 1680

Introduction 1680
clear ipv6 mld 1682
clear ipv6 mld group 1683
clear ipv6 mld interface 1684
debug mld 1685
ipv6 mld 1686
ipv6 mld access-group 1687
ipv6 mld immediate-leave 1688
ipv6 mld last-member-query-count 1689
ipv6 mld last-member-query-interval 1690
ipv6 mld limit 1691
ipv6 mld querier-timeout 1693

ipv6 mld query-interval 1694
ipv6 mld query-max-response-time 1695
ipv6 mld robustness-variable 1696
ipv6 mld snooping 1697
ipv6 mld snooping fast-leave 1699
ipv6 mld snooping mrouter 1700
ipv6 mld snooping querier 1702
ipv6 mld snooping report-suppression 1703
ipv6 mld ssm-map enable 1705
ipv6 mld ssm-map static 1706
ipv6 mld static-group 1707
ipv6 mld version 1709
show debugging mld 1710
show ipv6 mld groups 1711
show ipv6 mld interface 1712
show ipv6 mld snooping mrouter 1713
show ipv6 mld snooping statistics 1714

Chapter 34: Multicast Commands 1715
Introduction 1715
clear ip mroute 1717
clear ip mroute statistics 1718
clear ipv6 mroute 1719
clear ipv6 mroute statistics 1720
ipv6 multicast forward-slow-path-packet 1721
debug nsm 1722
debug nsm mcast 1723
debug nsm mcast6 1724
ip mroute 1725
ip multicast allow-register-fragments 1727
ip multicast forward-first-packet 1728
ip multicast route 1729
ip multicast route-limit 1731
ip multicast wrong-vif-suppression 1732
ip multicast-routing 1733
ipv6 mroute 1734
ipv6 multicast route 1736
ipv6 multicast route-limit 1739
ipv6 multicast-routing 1740
multicast 1741
platform multicast-ratelimit 1742
show debugging nsm mcast 1743
show ip mroute 1744
show ip mvif 1747
show ip rpf 1748
show ipv6 mroute 1749
show ipv6 multicast forwarding 1751
show ipv6 mif 1752

Chapter 35: PIM-SM Commands 1753
Introduction 1753
clear ip pim sparse-mode bsr rp-set * 1755

clear ip pim sparse-mode packet statistics 1756
clear ip mroute pim sparse-mode 1757
debug pim sparse-mode 1758
debug pim sparse-mode timer 1759
ip multicast allow-register-fragments 1761
ip pim accept-register list 1762
ip pim anycast-rp 1763
ip pim bsr-border 1764
ip pim bsr-candidate 1765
ip pim cisco-register-checksum 1766
ip pim cisco-register-checksum group-list 1767
ip pim crp-cisco-prefix 1768
ip pim dr-priority 1769
ip pim exclude-genid 1770
ip pim ext-srcs-directly-connected 1771
ip pim hello-holdtime (PIM-SM) 1772
ip pim hello-interval (PIM-SM) 1773
ip pim ignore-rp-set-priority 1774
ip pim jp-timer 1775
ip pim neighbor-filter (PIM-SM) 1776
ip pim register-rate-limit 1777
ip pim register-rp-reachability 1778
ip pim register-source 1779
ip pim register-suppression 1780
ip pim rp-address 1781
ip pim rp-candidate 1783
ip pim rp-register-kat 1785
ip pim sparse-mode 1786
ip pim sparse-mode join-prune-batching 1787
ip pim sparse-mode passive 1788
ip pim sparse-mode wrong-vif-suppression 1789
ip pim spt-threshold 1790
ip pim spt-threshold group-list 1791
ip pim ssm 1792
service pim 1793
show debugging pim sparse-mode 1794
show ip pim sparse-mode bsr-router 1795
show ip pim sparse-mode interface 1796
show ip pim sparse-mode interface detail 1798
show ip pim sparse-mode local-members 1799
show ip pim sparse-mode mroute 1800
show ip pim sparse-mode mroute detail 1802
show ip pim sparse-mode neighbor 1804
show ip pim sparse-mode nexthop 1805
show ip pim sparse-mode packet statistics 1806
show ip pim sparse-mode rp-hash 1807
show ip pim sparse-mode rp mapping 1808
undebug all pim sparse-mode 1809

Chapter 36: PIM-SMv6 Commands 1810

Introduction 1810
clear ipv6 mroute pim 1813
clear ipv6 mroute pim sparse-mode 1814

clear ipv6 pim sparse-mode bsr rp-set * 1815
debug ipv6 pim sparse-mode 1816
debug ipv6 pim sparse-mode packet 1818
debug ipv6 pim sparse-mode timer 1819
ipv6 pim accept-register 1821
ipv6 pim anycast-rp 1822
ipv6 pim bsr-border 1823
ipv6 pim bsr-candidate 1824
ipv6 pim cisco-register-checksum 1825
ipv6 pim cisco-register-checksum group-list 1826
ipv6 pim crp-cisco-prefix 1827
ipv6 pim dr-priority 1828
ipv6 pim exclude-genid 1829
ipv6 pim ext-srcs-directly-connected 1830
ipv6 pim hello-holdtime 1831
ipv6 pim hello-interval 1832
ipv6 pim ignore-rp-set-priority 1833
ipv6 pim jp-timer 1834
ipv6 pim neighbor-filter 1835
ipv6 pim register-rate-limit 1836
ipv6 pim register-rp-reachability 1837
ipv6 pim register-source 1838
ipv6 pim register-suppression 1839
ipv6 pim rp-address 1840
ipv6 pim rp-candidate 1842
ipv6 pim rp embedded 1844
ipv6 pim rp-register-kat 1845
ipv6 pim sparse-mode 1846
ipv6 pim sparse-mode passive 1847
ipv6 pim spt-threshold 1848
ipv6 pim spt-threshold group-list 1849
ipv6 pim ssm 1850
ipv6 pim unicast-bsm 1851
service pim6 1852
show debugging ipv6 pim sparse-mode 1853
show ipv6 pim sparse-mode bsr-router 1854
show ipv6 pim sparse-mode interface 1855
show ipv6 pim sparse-mode interface detail 1857
show ipv6 pim sparse-mode local-members 1858
show ipv6 pim sparse-mode mroute 1860
show ipv6 pim sparse-mode mroute detail 1862
show ipv6 pim sparse-mode neighbor 1864
show ipv6 pim sparse-mode nexthop 1865
show ipv6 pim sparse-mode rp-hash 1866
show ipv6 pim sparse-mode rp mapping 1867
show ipv6 pim sparse-mode rp nexthop 1868
undebug all ipv6 pim sparse-mode 1870
undebug ipv6 pim sparse-mode 1871

Chapter 37: PIM-DM Commands 1873

Introduction 1873
debug pim dense-mode all 1875
debug pim dense-mode context 1876

debug pim dense-mode decode 1877
debug pim dense-mode encode 1878
debug pim dense-mode fsm 1879
debug pim dense-mode mrt 1880
debug pim dense-mode nexthop 1881
debug pim dense-mode nsm 1882
debug pim dense-mode vif 1883
ip pim dense-mode 1884
ip pim dense-mode passive 1885
ip pim dense-mode wrong-vif-suppression 1886
ip pim ext-srcs-directly-connected 1887
ip pim hello-holdtime (PIM-DM) 1888
ip pim hello-interval (PIM-DM) 1889
ip pim max-graft-retries 1890
ip pim neighbor-filter (PIM-DM) 1892
ip pim propagation-delay 1893
ip pim state-refresh origination-interval 1894
service pdm 1895
show debugging pim dense-mode 1896
show ip pim dense-mode interface 1897
show ip pim dense-mode interface detail 1899
show ip pim dense-mode mroute 1900
show ip pim dense-mode neighbor 1901
show ip pim dense-mode neighbor detail 1902
show ip pim dense-mode nexthop 1903
undebug all pim dense-mode 1904

PART 5: Access and Security 1905

Chapter 38: IPv4 Hardware Access Control List (ACL) Commands 1906
Introduction 1906
access-group 1909
access-list (numbered hardware ACL for ICMP) 1911
access-list (numbered hardware ACL for IP packets) 1915
access-list (numbered hardware ACL for IP protocols) 1918
access-list (numbered hardware ACL for MAC addresses) 1923
access-list (numbered hardware ACL for TCP or UDP) 1926
access-list hardware (named hardware ACL) 1930
acl-group ip address 1932
acl-group ip port 1933
(acl-group ip port range) 1934
commit (IPv4) 1936
ip (ip-host-group) 1937
(named hardware ACL entry for ICMP) 1939
(named hardware ACL entry for IP packets) 1943
(named hardware ACL entry for IP protocols) 1947
(named hardware ACL entry for MAC addresses) 1952
(named hardware ACL entry for TCP or UDP) 1955
show access-group 1959
show access-list (IPv4 Hardware ACLs) 1960
show acl-group ip address 1962
show acl-group ip port 1963

show interface access-group 1964

Chapter 39: IPv4 Software Access Control List (ACL) Commands 1965

Introduction 1965
access-list extended (named) 1968
access-list (extended numbered) 1976
(access-list extended ICMP filter) 1979
(access-list extended IP filter) 1981
(access-list extended IP protocol filter) 1984
(access-list extended TCP UDP filter) 1988
access-list standard (named) 1991
access-list (standard numbered) 1993
(access-list standard named filter) 1995
(access-list standard numbered filter) 1997
clear ip prefix-list 1999
dos 2000
ip prefix-list 2003
maximum-access-list (deleted) 2005
show access-list (IPv4 Software ACLs) 2006
show dos interface 2008
show ip access-list 2011
show ip prefix-list 2012
vty access-class (numbered) 2013

Chapter 40: IPv6 Hardware Access Control List (ACL) Commands 2014

Introduction 2014
acl-group ipv6 address 2016
commit (IPv6) 2017
ipv6 (ipv6-host-group) 2018
ipv6 access-list (named IPv6 hardware ACL) 2020
ipv6 traffic-filter 2022
(named IPv6 hardware ACL: ICMP entry) 2023
(named IPv6 hardware ACL: IPv6 packet entry) 2027
(named IPv6 hardware ACL: IP protocol entry) 2030
(named IPv6 hardware ACL: TCP or UDP entry) 2035
show acl-group ipv6 address 2039
show ipv6 access-list (IPv6 Hardware ACLs) 2040

Chapter 41: IPv6 Software Access Control List (ACL) Commands 2041

Introduction 2041
ipv6 access-list extended (named) 2043
ipv6 access-list extended proto 2047
(ipv6 access-list extended IP protocol filter) 2050
(ipv6 access-list extended TCP UDP filter) 2053
ipv6 access-list standard (named) 2055
(ipv6 access-list standard filter) 2057
ipv6 prefix-list 2059
show ipv6 access-list (IPv6 Software ACLs) 2061
show ipv6 prefix-list 2063
vty ipv6 access-class (named) 2064

Chapter 42: QoS Commands 2065

Introduction 2065
class 2067
class-map 2068
clear mls qos interface policer-counters 2069
default-action 2070
description (QoS policy-map) 2071
egress-rate-limit 2072
egress-rate-limit overhead 2074
match access-group 2075
match cos 2077
match dscp 2078
match eth-format protocol 2079
match inner-cos 2082
match inner-vlan 2083
match ip-precedence 2084
match mac-type 2085
match tcp-flags 2086
match vlan 2087
mls qos cos 2088
mls qos enable 2089
mls qos map cos-queue 2090
mls qos map premark-dscp 2091
no police 2093
police single-rate action 2094
police twin-rate action 2096
policy-map 2098
priority-queue 2099
remark-map 2100
remark new-cos 2102
service-policy input 2104
show class-map 2105
show mls qos 2106
show mls qos interface 2107
show mls qos interface policer-counters 2110
show mls qos interface queue-counters 2111
show mls qos interface storm-status 2112
show mls qos maps cos-queue 2113
show mls qos maps premark-dscp 2114
show platform classifier statistics utilization brief 2115
show policy-map 2117
storm-action 2118
storm-downtime 2119
storm-protection 2120
storm-rate 2121
storm-window 2122
trust dscp 2123
wrr-queue disable queues 2124
wrr-queue egress-rate-limit queues 2125
wrr-queue weight queues 2126

Chapter 43: 802.1X Commands 2127

Introduction 2127
dot1x accounting 2129

dot1x authentication 2130
debug dot1x 2131
dot1x control-direction 2132
dot1x eap 2134
dot1x eapol-version 2135
dot1x initialize interface 2136
dot1x initialize supplicant 2137
dot1x keytransmit 2138
dot1x max-auth-fail 2139
dot1x max-reauth-req 2141
dot1x port-control 2143
dot1x timeout tx-period 2145
show debugging dot1x 2147
show dot1x 2148
show dot1x diagnostics 2151
show dot1x interface 2153
show dot1x sessionstatistics 2155
show dot1x statistics interface 2156
show dot1x supplicant 2157
show dot1x supplicant interface 2159
undebug dot1x 2161

Chapter 44: Authentication Commands 2162

Introduction 2162
auth auth-fail vlan 2166
auth critical 2168
auth dhcp-framed-ip-lease 2169
auth dynamic-vlan-creation 2171
auth guest-vlan 2174
auth guest-vlan forward 2176
auth guest-vlan hw-forwarding 2178
auth host-mode 2179
auth log 2181
auth max-supplicant 2183
auth multi-vlan-session 2185
auth priority 2186
auth profile (global) 2188
auth profile (interface) 2189
auth reauthentication 2190
auth roaming disconnected 2191
auth roaming enable 2193
auth supplicant-ip 2195
auth supplicant-mac 2197
auth timeout connect-timeout 2200
auth timeout quiet-period 2201
auth timeout reauth-period 2202
auth timeout server-timeout 2204
auth timeout supp-timeout 2206
auth two-step enable 2207
auth two-step order 2210
auth-mac accounting 2212
auth-mac authentication 2213
auth-mac enable 2214

auth-mac method 2216
auth-mac password 2218
auth-mac reauth-relearning 2219
auth-mac static 2220
auth-mac username 2221
auth-web accounting 2222
auth-web authentication 2223
auth-web enable 2224
auth-web forward 2226
auth-web idle-timeout enable 2229
auth-web idle-timeout timeout 2230
auth-web max-auth-fail 2231
auth-web method 2233
auth-web-server blocking-mode 2234
auth-web-server dhcp ipaddress 2235
auth-web-server dhcp lease 2236
auth-web-server dhcp-wpad-option 2237
auth-web-server host-name 2238
auth-web-server intercept-port 2239
auth-web-server ipaddress 2240
auth-web-server page language 2241
auth-web-server login-url 2242
auth-web-server page logo 2243
auth-web-server page sub-title 2244
auth-web-server page success-message 2245
auth-web-server page title 2246
auth-web-server page welcome-message 2247
auth-web-server ping-poll enable 2248
auth-web-server ping-poll failcount 2249
auth-web-server ping-poll interval 2250
auth-web-server ping-poll reauth-timer-refresh 2251
auth-web-server ping-poll timeout 2252
auth-web-server port 2253
auth-web-server redirect-delay-time 2254
auth-web-server redirect-url 2255
auth-web-server session-keep 2256
auth-web-server ssl 2257
auth-web-server ssl intercept-port 2258
copy proxy-autoconfig-file 2259
copy web-auth-https-file 2260
description (auth-profile) 2261
erase proxy-autoconfig-file 2262
erase web-auth-https-file 2263
platform l3-vlan-hashing-algorithm 2264
platform mac-vlan-hashing-algorithm 2265
show auth 2266
show auth diagnostics 2268
show auth interface 2270
show auth sessionstatistics 2272
show auth statistics interface 2273
show auth supplicant 2274
show auth supplicant interface 2277
show auth two-step supplicant brief 2278

show auth-web-server 2280
show auth-web-server page 2281
show proxy-autoconfig-file 2282

Chapter 45: AAA Commands 2283
Introduction 2283
aaa accounting auth-mac 2285
aaa accounting auth-web 2287
aaa accounting commands 2289
aaa accounting dot1x 2291
aaa accounting login 2293
aaa accounting update 2296
aaa authentication auth-mac 2298
aaa authentication auth-web 2300
aaa authentication dot1x 2302
aaa authentication enable default group tacacs+ 2304
aaa authentication enable default local 2306
aaa authentication login 2307
aaa authorization commands 2309
aaa authorization config-commands 2311
aaa group server 2312
aaa local authentication attempts lockout-time 2314
aaa local authentication attempts max-fail 2315
aaa login fail-delay 2316
accounting login 2317
authorization commands 2318
clear aaa local user lockout 2320
debug aaa 2321
login authentication 2322
proxy-port 2323
radius-secure-proxy aaa 2324
server (radsecproxy-aaa) 2325
server mutual-authentication 2327
server name-check 2328
server trustpoint 2329
show aaa local user locked 2331
show aaa server group 2332
show debugging aaa 2333
show radius server group 2334
undebug aaa 2336

Chapter 46: RADIUS Commands 2337
Introduction 2337
auth radius send nas-identifier 2338
auth radius send service-type 2339
deadtime (RADIUS server group) 2340
debug radius 2341
ip radius source-interface 2342
radius-server deadtime 2343
radius-server host 2344
radius-server key 2348
radius-server retransmit 2350

radius-server timeout 2352
server (server group) 2354
show debugging radius 2356
show radius 2357
show radius statistics 2360
undebug radius 2361

Chapter 47: Local RADIUS Server Commands 2362
Introduction 2362
attribute 2364
authentication 2366
client (radsecproxy-srv) 2367
client mutual-authentication 2369
client name-check 2370
client trustpoint 2371
clear radius local-server statistics 2372
copy fdb-radius-users (to file) 2373
copy local-radius-user-db (from file) 2375
copy local-radius-user-db (to file) 2376
crypto pki enroll local (deleted) 2377
crypto pki enroll local local-radius-all-users (deleted) 2378
crypto pki enroll local user (deleted) 2379
crypto pki export local pem (deleted) 2380
crypto pki export local pkcs12 (deleted) 2381
crypto pki trustpoint local (deleted) 2382
debug crypto pki (deleted) 2383
domain-style 2384
egress-vlan-id 2385
egress-vlan-name 2387
group 2389
nas 2390
help radius-attribute 2391
radius-secure-proxy local-server 2393
radius-server local 2394
server auth-port 2395
server enable 2396
show radius local-server group 2397
show radius local-server nas 2398
show radius local-server statistics 2399
show radius local-server user 2400
user (RADIUS server) 2402
vlan (RADIUS server) 2404

Chapter 48: Public Key Infrastructure and Crypto Commands 2405
Introduction 2405
crypto key generate rsa 2407
crypto key zeroize 2408
crypto pki authenticate 2409
crypto pki enroll 2410
crypto pki enroll user 2411
crypto pki export pem 2413
crypto pki export pkcs12 2414

crypto pki import pem 2416
crypto pki import pkcs12 2418
crypto pki trustpoint 2419
crypto secure-mode 2420
crypto secure-mode delete hostkey 2421
crypto verify 2422
enrollment (ca-trustpoint) 2424
fingerprint (ca-trustpoint) 2425
no crypto pki certificate 2427
rsakeypair (ca-trustpoint) 2428
show crypto key mypubkey rsa 2429
show crypto pki certificates 2430
show crypto pki enrollment user 2432
show crypto pki trustpoint 2433
show secure-mode 2434
subject-name (ca-trustpoint) 2435

Chapter 49: TACACS+ Commands 2437
Introduction 2437
aaa authorization commands 2438
aaa authorization config-commands 2440
authorization commands 2441
ip tacacs source-interface 2443
show tacacs+ 2444
tacacs-server host 2446
tacacs-server key 2448
tacacs-server timeout 2449

Chapter 50: DHCP Snooping Commands 2450
Introduction 2450
arp security 2452
arp security drop link-local-arps 2453
arp security violation 2454
clear arp security statistics 2456
clear ip dhcp snooping binding 2457
clear ip dhcp snooping statistics 2458
debug arp security 2459
debug ip dhcp snooping 2460
ip dhcp snooping 2461
ip dhcp snooping agent-option 2463
ip dhcp snooping agent-option allow-untrusted 2464
ip dhcp snooping agent-option circuit-id vlantriplet 2465
ip dhcp snooping agent-option remote-id 2466
ip dhcp snooping binding 2467
ip dhcp snooping database 2468
ip dhcp snooping delete-by-client 2469
ip dhcp snooping delete-by-linkdown 2470
ip dhcp snooping max-bindings 2471
ip dhcp snooping subscriber-id 2472
ip dhcp snooping trust 2473
ip dhcp snooping verify mac-address 2474
ip dhcp snooping violation 2475

ip source binding 2476
service dhcp-snooping 2478
show arp security 2480
show arp security interface 2481
show arp security statistics 2483
show debugging arp security 2485
show debugging ip dhcp snooping 2486
show ip dhcp snooping 2487
show ip dhcp snooping acl 2488
show ip dhcp snooping agent-option 2491
show ip dhcp snooping binding 2493
show ip dhcp snooping interface 2495
show ip dhcp snooping statistics 2497
show ip source binding 2500

Chapter 51: OpenFlow Commands 2501
Introduction 2501
openflow 2502
openflow controller 2503
openflow datapath-id 2505
openflow failmode 2506
openflow inactivity 2508
openflow native vlan 2509
openflow ssl peer certificate 2510
openflow ssl trustpoint 2511
openflow version 2512
show openflow config 2513
show openflow coverage 2515
show openflow flows 2517
show openflow rules 2520
show openflow ssl 2522
show openflow status 2523

PART 6: Network Availability 2526

Chapter 52: VRRP Commands 2527
Introduction 2527
advertisement-interval 2529
alternate-checksum-mode 2531
circuit-failover 2532
debug vrrp 2534
debug vrrp events 2535
debug vrrp packet 2536
disable (VRRP) 2537
enable (VRRP) 2538
preempt-mode 2539
priority 2541
router ipv6 vrrp (interface) 2543
router vrrp (interface) 2545
show debugging vrrp 2547
show running-config router ipv6 vrrp 2548
show running-config router vrrp 2549

show vrrp 2550
show vrrp counters 2552
show vrrp ipv6 2555
show vrrp (session) 2556
transition-mode 2558
undebug vrrp 2560
undebug vrrp events 2561
undebug vrrp packet 2562
virtual-ip 2563
virtual-ipv6 2565
vrrp vmac 2567

Chapter 53: Ethernet Protection Switched Ring (EPSRing™) Commands 2568
Introduction 2568
debug epsr 2570
epsr 2571
epsr configuration 2572
epsr datavlan 2573
epsr enhancedrecovery enable 2574
epsr flush-type 2575
epsr mode master controlvlan primary port 2577
epsr mode transit controlvlan 2578
epsr priority 2579
epsr state 2580
epsr topology-change 2581
epsr trap 2582
show debugging epsr 2583
show epsr 2584
show epsr common segments 2589
show epsr config-check 2590
show epsr <epsr-instance> 2591
show epsr <epsr-instance> counters 2592
show epsr counters 2593
show epsr summary 2594
undebug epsr 2595

Chapter 54: G.8032 Ethernet Ring Protection Switching Commands 2596
Introduction 2596
cfm-sf-notify 2598
clear g8032 erp-instance 2600
clear g8032 erp-instance statistics 2602
data-traffic 2603
debug g8032 2605
enable (g8032-profile) 2606
epsr topology-change 2607
erp-instance 2608
g8032 erp-instance 2609
g8032 forced-switch erp-instance 2611
g8032 manual-switch erp-instance 2613
g8032 physical-ring 2614
g8032 profile 2616
level (g8032-switch) 2617

physical-ring 2618
profile name 2619
raps-channel 2620
service onm 2621
rpl role 2622
show debugging g8032 2624
show g8032 erp-instance 2625
show g8032 erp-instance statistics 2630
show g8032 physical-ring 2632
show g8032 profile 2634
sub-ring 2636
timer (g8032-profile) 2637
topology-change 2639
trap (g8032-switch) 2641
undebug g8032 2642

Chapter 55: Media Redundancy Protocol (MRP) Commands 2643
Introduction 2643
clear counter mrp 2644
debug mrp 2645
domain-id (mrp-ring) 2646
domain-name (mrp-ring) 2647
enable (mrp-ring) 2648
lc-react 2649
mrp ring 2650
profile (mrp-ring) 2652
role (mrp-ring) 2653
service mrp 2654
show counter mrp 2655
show debugging mrp 2659
show mrp ports 2660
show mrp ring 2661
vlan-id (mrp-ring) 2663

PART 7: Network Management 2664

Chapter 56: Allied Telesis Management Framework™ (AMF) Commands 2665
Introduction 2665
application-proxy ip-filter 2671
application-proxy quarantine-vlan 2672
application-proxy redirect-url 2673
application-proxy threat-protection 2674
application-proxy threat-protection send-summary 2675
application-proxy whitelist advertised-address 2676
application-proxy whitelist enable 2677
application-proxy whitelist protection tls 2678
application-proxy whitelist server 2679
application-proxy whitelist trustpoint (deprecated) 2681
area-link 2682
atmf-arealink 2684
atmf-link 2686
atmf area 2687

atmf area password 2689
atmf authorize 2691
atmf authorize provision 2693
atmf backup 2695
atmf backup area-masters delete 2696
atmf backup area-masters enable 2697
atmf backup area-masters now 2698
atmf backup area-masters synchronize 2699
atmf backup bandwidth 2700
atmf backup delete 2701
atmf backup enable 2702
atmf backup guests delete 2703
atmf backup guests enable 2704
atmf backup guests now 2705
atmf backup guests synchronize 2706
atmf backup now 2707
atmf backup redundancy enable 2709
atmf backup server 2710
atmf backup stop 2712
atmf backup synchronize 2713
atmf cleanup 2714
atmf container 2715
atmf container login 2716
atmf controller 2717
atmf distribute firmware 2718
atmf domain vlan 2720
atmf enable 2723
atmf group (membership) 2724
atmf guest-class 2726
atmf log-verbose 2728
atmf management subnet 2729
atmf management vlan 2732
atmf master 2734
atmf mtu 2735
atmf network-name 2736
atmf provision (interface) 2737
atmf provision node 2738
atmf reboot-rolling 2740
atmf recover 2744
atmf recover guest 2746
atmf recover led-off 2747
atmf recover over-eth 2748
atmf recovery-server 2749
atmf remote-login 2751
atmf restricted-login 2753
atmf retry guest-link 2755
atmf secure-mode 2756
atmf secure-mode certificate expire 2758
atmf secure-mode certificate expiry 2759
atmf secure-mode certificate renew 2760
atmf secure-mode enable-all 2761
atmf select-area 2763
atmf topology-gui enable 2764

atmf trustpoint . . . 2765
atmf virtual-crosslink . . . 2767
atmf virtual-link . . . 2769
atmf virtual-link description . . . 2772
atmf virtual-link protection . . . 2773
atmf working-set . . . 2775
bridge-group . . . 2777
clear application-proxy threat-protection . . . 2778
clear atmf links . . . 2779
clear atmf links virtual . . . 2780
clear atmf links statistics . . . 2781
clear atmf recovery-file . . . 2782
clear atmf secure-mode certificates . . . 2783
clear atmf secure-mode statistics . . . 2784
clone (amf-provision) . . . 2785
configure boot config (amf-provision) . . . 2787
configure boot system (amf-provision) . . . 2789
copy (amf-provision) . . . 2791
create (amf-provision) . . . 2792
debug atmf . . . 2794
debug atmf packet . . . 2796
delete (amf-provision) . . . 2799
discovery . . . 2801
description (amf-container) . . . 2803
erase factory-default . . . 2804
http-enable . . . 2805
identity (amf-provision) . . . 2807
license-cert (amf-provision) . . . 2809
locate (amf-provision) . . . 2811
log event-host . . . 2813
login-fallback enable . . . 2814
modeltype . . . 2815
service atmf-application-proxy . . . 2816
show application-proxy threat-protection . . . 2817
show application-proxy whitelist advertised-address . . . 2819
show application-proxy whitelist interface . . . 2820
show application-proxy whitelist server . . . 2822
show application-proxy whitelist supplicant . . . 2823
show atmf . . . 2825
show atmf area . . . 2829
show atmf area guests . . . 2832
show atmf area guests-detail . . . 2834
show atmf area nodes . . . 2836
show atmf area nodes-detail . . . 2838
show atmf area summary . . . 2840
show atmf authorization . . . 2841
show atmf backup . . . 2844
show atmf backup area . . . 2848
show atmf backup guest . . . 2850
show atmf container . . . 2852
show atmf detail . . . 2855
show atmf group . . . 2857
show atmf group members . . . 2859

show atmf guests 2861
show atmf guests detail 2863
show atmf links 2866
show atmf links detail 2868
show atmf links guest 2877
show atmf links guest detail 2879
show atmf links statistics 2883
show atmf nodes 2886
show atmf provision nodes 2888
show atmf recovery-file 2890
show atmf secure-mode 2891
show atmf secure-mode audit 2893
show atmf secure-mode audit link 2894
show atmf secure-mode certificates 2895
show atmf secure-mode sa 2898
show atmf secure-mode statistics 2901
show atmf tech 2903
show atmf virtual-links 2906
show atmf working-set 2908
show debugging atmf 2909
show debugging atmf packet 2910
show running-config atmf 2911
state 2912
switchport atmf-agentlink 2914
switchport atmf-arealink 2915
switchport atmf-crosslink 2917
switchport atmf-guestlink 2919
switchport atmf-link 2921
type atmf node 2922
undebug atmf 2925
username 2926

Chapter 57: Dynamic Host Configuration Protocol (DHCP) Commands 2927

Introduction 2927
bootfile 2929
clear ip dhcp binding 2930
default-router 2931
dns-server 2932
domain-name 2933
host (DHCP) 2934
ip address dhcp 2935
ip dhcp bootp ignore 2937
ip dhcp leasequery enable 2938
ip dhcp option 2939
ip dhcp pool 2941
ip dhcp-client default-route distance 2942
ip dhcp-client request vendor-identifying-specific 2944
ip dhcp-client vendor-identifying-class 2945
ip dhcp-relay agent-option 2946
ip dhcp-relay agent-option checking 2948
ip dhcp-relay agent-option remote-id 2949
ip dhcp-relay information policy 2950
ip dhcp-relay maxhops 2952

ip dhcp-relay max-message-length . . . 2953
ip dhcp-relay server-address . . . 2955
ip dhcp-relay use-client-side-address . . . 2957
lease . . . 2959
network (DHCP) . . . 2961
next-server . . . 2962
option . . . 2963
probe enable . . . 2965
probe packets . . . 2966
probe timeout . . . 2967
probe type . . . 2968
range . . . 2969
route . . . 2970
service dhcp-relay . . . 2971
service dhcp-server . . . 2972
short-lease-threshold . . . 2973
show counter dhcp-client . . . 2975
show counter dhcp-relay . . . 2976
show counter dhcp-server . . . 2979
show dhcp lease . . . 2981
show ip dhcp binding . . . 2982
show ip dhcp pool . . . 2983
show ip dhcp-relay . . . 2988
show ip dhcp server statistics . . . 2989
show ip dhcp server summary . . . 2991
subnet-mask . . . 2992

Chapter 58: DHCP for IPv6 (DHCPv6) Commands . . . 2993
Introduction . . . 2993
clear counter ipv6 dhcp-client . . . 2995
clear ipv6 dhcp client . . . 2996
ip dhcp-relay agent-option . . . 2997
ip dhcp-relay agent-option subscriber-id-auto-mac . . . 2999
ip dhcp-relay agent-option checking . . . 3000
ip dhcp-relay agent-option remote-id . . . 3001
ip dhcp-relay information policy . . . 3002
ip dhcp-relay maxhops . . . 3004
ip dhcp-relay max-message-length . . . 3005
ip dhcp-relay server-address . . . 3007
ipv6 address dhcp . . . 3009
service dhcp-relay . . . 3011
show counter dhcp-relay . . . 3012
show counter ipv6 dhcp-client . . . 3015
show ip dhcp-relay . . . 3017
show ipv6 dhcp . . . 3018
show ipv6 dhcp interface . . . 3019

Chapter 59: NTP Commands . . . 3020
Introduction . . . 3020
ntp authentication-key . . . 3021
ntp broadcastdelay . . . 3023
ntp master . . . 3024

ntp peer . . . 3025
ntp rate-limit . . . 3027
ntp restrict . . . 3028
ntp server . . . 3030
ntp source . . . 3032
show ntp associations . . . 3034
show ntp counters . . . 3036
show ntp counters associations . . . 3037
show ntp status . . . 3038

Chapter 60: Precision Time Protocol (PTP) and Transparent Clock Commands . . . 3039
Introduction . . . 3039
clock-port . . . 3040
ptp-clk . . . 3041
ptp global . . . 3043
show ptp data transparent . . . 3044
show ptp port . . . 3045

Chapter 61: SNMP Commands . . . 3046
Introduction . . . 3046
alias (interface) . . . 3048
debug snmp . . . 3049
show counter snmp-server . . . 3050
show debugging snmp . . . 3054
show running-config snmp . . . 3055
show snmp-server . . . 3056
show snmp-server community . . . 3057
show snmp-server group . . . 3058
show snmp-server user . . . 3059
show snmp-server view . . . 3060
snmp trap link-status . . . 3061
snmp trap link-status suppress . . . 3062
snmp-server . . . 3064
snmp-server community . . . 3066
snmp-server contact . . . 3067
snmp-server enable trap . . . 3068
snmp-server engineID local . . . 3071
snmp-server engineID local reset . . . 3073
snmp-server group . . . 3074
snmp-server host . . . 3076
snmp-server legacy-ifadminstatus . . . 3078
snmp-server location . . . 3079
snmp-server source-interface . . . 3080
snmp-server startup-trap-delay . . . 3081
snmp-server user . . . 3082
snmp-server view . . . 3085
undebug snmp . . . 3086

Chapter 62: LLDP Commands . . . 3087
Introduction . . . 3087
clear lldp statistics . . . 3089
clear lldp table . . . 3090

debug lldp . . . 3091
lldp faststart-count . . . 3093
lldp holdtime-multiplier . . . 3094
lldp management-address . . . 3095
lldp med-notifications . . . 3096
lldp med-tlv-select . . . 3097
lldp non-strict-med-tlv-order-check . . . 3100
lldp notification-interval . . . 3101
lldp notifications . . . 3102
lldp port-number-type . . . 3103
lldp reinit . . . 3104
lldp run . . . 3105
lldp timer . . . 3106
lldp tlv-select . . . 3107
lldp transmit receive . . . 3109
lldp tx-delay . . . 3110
location civic-location configuration . . . 3111
location civic-location identifier . . . 3115
location civic-location-id . . . 3116
location coord-location configuration . . . 3117
location coord-location identifier . . . 3119
location coord-location-id . . . 3120
location elin-location . . . 3122
location elin-location-id . . . 3123
show debugging lldp . . . 3124
show lldp . . . 3126
show lldp interface . . . 3128
show lldp local-info . . . 3130
show lldp neighbors . . . 3135
show lldp neighbors detail . . . 3137
show lldp statistics . . . 3141
show lldp statistics interface . . . 3143
show location . . . 3145

Chapter 63: Mail (SMTP) Commands . . . 3147

Introduction . . . 3147
debug mail . . . 3148
delete mail . . . 3149
mail . . . 3150
mail from . . . 3152
mail smtpserver . . . 3153
mail smtpserver authentication . . . 3154
mail smtpserver port . . . 3156
show counter mail . . . 3158
show mail . . . 3159
undebug mail . . . 3160

Chapter 64: RMON Commands . . . 3161

Introduction . . . 3161
rmon alarm . . . 3162
rmon collection history . . . 3165
rmon collection stats . . . 3166

rmon event . . . 3167
show rmon alarm . . . 3168
show rmon event . . . 3169
show rmon history . . . 3171
show rmon statistics . . . 3173

Chapter 65: Secure Shell (SSH) Commands . . . 3175
Introduction . . . 3175
banner login (SSH) . . . 3177
clear ssh . . . 3178
crypto key destroy hostkey . . . 3179
crypto key destroy userkey . . . 3180
crypto key generate hostkey . . . 3181
crypto key generate userkey . . . 3183
crypto key pubkey-chain knownhosts . . . 3184
crypto key pubkey-chain userkey . . . 3186
debug ssh client . . . 3188
debug ssh server . . . 3189
service ssh . . . 3190
show banner login . . . 3192
show crypto key hostkey . . . 3193
show crypto key pubkey-chain knownhosts . . . 3195
show crypto key pubkey-chain userkey . . . 3196
show crypto key userkey . . . 3197
show running-config ssh . . . 3198
show ssh . . . 3200
show ssh client . . . 3202
show ssh server . . . 3203
show ssh server allow-users . . . 3205
show ssh server deny-users . . . 3206
ssh . . . 3207
ssh client . . . 3210
ssh server . . . 3212
ssh server allow-users . . . 3214
ssh server authentication . . . 3216
ssh server deny-users . . . 3218
ssh server max-auth-tries . . . 3220
ssh server resolve-host . . . 3221
ssh server scp . . . 3222
ssh server secure-ciphers . . . 3223
ssh server secure-kex . . . 3224
ssh server sftp . . . 3226
undebug ssh client . . . 3227
undebug ssh server . . . 3228

Chapter 66: Trigger Commands . . . 3229
Introduction . . . 3229
active (trigger) . . . 3231
day . . . 3232
debug trigger . . . 3234
description (trigger) . . . 3235
repeat . . . 3236

script . . . 3237
show debugging trigger . . . 3239
show running-config trigger . . . 3240
show trigger . . . 3241
test . . . 3246
time (trigger) . . . 3247
trap . . . 3249
trigger . . . 3250
trigger activate . . . 3251
type atmf node . . . 3252
type cpu . . . 3255
type interface . . . 3256
type linkmon-probe . . . 3257
type log . . . 3259
type memory . . . 3260
type periodic . . . 3261
type ping-poll . . . 3262
type reboot . . . 3263
type time . . . 3264
type usb . . . 3265
undebug trigger . . . 3266

Chapter 67: Ping-Polling Commands . . . 3267
Introduction . . . 3267
active (ping-polling) . . . 3269
clear ping-poll . . . 3270
critical-interval . . . 3271
debug ping-poll . . . 3272
description (ping-polling) . . . 3273
fail-count . . . 3274
ip (ping-polling) . . . 3275
length (ping-poll data) . . . 3276
normal-interval . . . 3277
ping-poll . . . 3278
sample-size . . . 3279
show counter ping-poll . . . 3281
show ping-poll . . . 3283
source-ip . . . 3287
timeout (ping polling) . . . 3289
up-count . . . 3290
undebug ping-poll . . . 3291

Chapter 68: sFlow Commands . . . 3292
Introduction . . . 3292
debug sflow . . . 3293
debug sflow agent . . . 3294
sflow agent . . . 3295
sflow collector . . . 3297
sflow collector max-datagram-size . . . 3299
sflow enable . . . 3300
sflow max-header-size . . . 3301
sflow polling-interval . . . 3303

sflow sampling-rate 3304
show debugging sflow 3305
show running-config sflow 3307
show sflow 3308
show sflow interface 3310
undebug sflow 3311

Chapter 69: MODBUS Commands 3312
Introduction 3312
clear scada modbus tcp server connection 3313
clear scada modbus tcp server statistics 3314
scada modbus tcp server access 3315
scada modbus tcp server access permit 3316
scada modbus tcp server connection 3317
scada modbus tcp server port 3318
scada modbus tcp server 3319
show scada modbus tcp server connections 3320
show scada modbus tcp server 3322

List of Commands

(access-list extended ICMP filter) 1979
(access-list extended IP filter) 1981
(access-list extended IP protocol filter) 1984
(access-list extended TCP UDP filter) 1988
(access-list standard named filter) 1995
(access-list standard numbered filter) 1997
(acl-group ip port range) 1934
(ipv6 access-list extended IP protocol filter) 2050
(ipv6 access-list extended TCP UDP filter) 2053
(ipv6 access-list standard filter) 2057
(named hardware ACL entry for ICMP) 1939
(named hardware ACL entry for IP packets) 1943
(named hardware ACL entry for IP protocols) 1947
(named hardware ACL entry for MAC addresses) 1952
(named hardware ACL entry for TCP or UDP) 1955
(named IPv6 hardware ACL: ICMP entry) 2023
(named IPv6 hardware ACL: IP protocol entry) 2030
(named IPv6 hardware ACL: IPv6 packet entry) 2027
(named IPv6 hardware ACL: TCP or UDP entry) 2035
aaa accounting auth-mac 2285
aaa accounting auth-web 2287
aaa accounting commands 2289
aaa accounting dot1x 2291
aaa accounting login 2293
aaa accounting update 2296

aaa authentication auth-mac....2298
aaa authentication auth-web 2300
aaa authentication dot1x 2302
aaa authentication enable default group tacacs+ 2304
aaa authentication enable default local....185
aaa authentication enable default local....2306
aaa authentication login 2307
aaa authorization commands 2309
aaa authorization commands 2438
aaa authorization config-commands 2311
aaa authorization config-commands 2440
aaa group server....2312
aaa local authentication attempts lockout-time....186
aaa local authentication attempts lockout-time....2314
aaa local authentication attempts max-fail 187
aaa local authentication attempts max-fail 2315
aaa login fail-delay....188
aaa login fail-delay....2316
abr-type....1182
accept-lifetime 988
access-group 1909
access-list (extended numbered)....1976
access-list (numbered hardware ACL for ICMP) 1911
access-list (numbered hardware ACL for IP packets)....1915
access-list (numbered hardware ACL for IP protocols)....1918
access-list (numbered hardware ACL for MAC addresses) 1923
access-list (numbered hardware ACL for TCP or UDP) 1926
access-list (standard numbered)....1993
access-list extended (named) 1968
access-list hardware (named hardware ACL)....1930
access-list standard (named) 1991
accounting login 2317
acl-group ip address 1932
acl-group ip port 1933
acl-group ipv6 address....2016

activate 476
active (ping-polling) 3269
active (trigger)....3231
address-family....1279
advertisement-interval....2529
aggregate-address (IPv6 RIPng) 1045
aggregate-address....1281
alarm facility epsr led 509
alarm facility epsr relay 510
alarm facility g8032 led 511
alarm facility g8032 relay....512
alarm facility input-alarm alarm-position 513
alarm facility input-alarm led....514
alarm facility input-alarm relay 516
alarm facility link-down led 518
alarm facility link-down relay....519
alarm facility loopprot led....520
alarm facility loopprot relay 521
alarm facility main-pse led 522
alarm facility main-pse relay 523
alarm facility power-supply led....524
alarm facility power-supply relay 525
alarm facility pse-port led 526
alarm facility pse-port relay 527
alarm facility temperature led 529
alarm facility temperature relay 530
alarm facility ufo led 531
alarm facility ufo relay 532
alias (interface) 3048
alliedware-behavior 990
alternate-checksum-mode 2531
application-proxy ip-filter 2671
application-proxy quarantine-vlan 2672
application-proxy redirect-url 2673
application-proxy threat-protection send-summary....2675

application-proxy threat-protection 2674
application-proxy whitelist advertised-address 2676
application-proxy whitelist enable 2677
application-proxy whitelist protection tls 2678
application-proxy whitelist server 2679
application-proxy whitelist trustpoint (deprecated) 2681
area authentication ipsec spi 1183
area authentication 1076
area default-cost (IPv6 OSPF) 1185
area default-cost 1075
area encryption ipsec spi esp 1186
area filter-list 1077
area nssa 1078
area range (IPv6 OSPF) 1189
area range 1080
area stub (IPv6 OSPF) 1191
area stub 1082
area virtual-link (IPv6 OSPF) 1192
area virtual-link authentication ipsec spi 1194
area virtual-link encryption ipsec spi 1196
area virtual-link 1083
area-link 2682
arp log 838
arp opportunistic-nd 841
arp security drop link-local-arps 2453
arp security violation 2454
arp security 2452
arp 836
arp-aging-timeout 832
arp-mac-disparity 833
arp-reply-bc-dmac 842
atmf area password 2689
atmf area 2687
atmf authorize provision 2693
atmf authorize 2691

atmf backup area-masters delete....2696
atmf backup area-masters enable....2697
atmf backup area-masters now....2698
atmf backup area-masters synchronize....2699
atmf backup bandwidth....2700
atmf backup delete....2701
atmf backup enable....2702
atmf backup guests delete....2703
atmf backup guests enable....2704
atmf backup guests now....2705
atmf backup guests synchronize....2706
atmf backup now....2707
atmf backup redundancy enable....2709
atmf backup server....2710
atmf backup stop....2712
atmf backup synchronize....2713
atmf backup....2695
atmf cleanup....2714
atmf container login....2716
atmf container....2715
atmf controller....2717
atmf distribute firmware....2718
atmf domain vlan....2720
atmf enable....2723
atmf group (membership)....2724
atmf guest-class....2726
atmf log-verbose....2728
atmf management subnet....2729
atmf management vlan....2732
atmf master....2734
atmf mtu....2735
atmf network-name....2736
atmf provision (interface)....2737
atmf provision node....2738
atmf reboot-rolling....2740

atmf recover guest. 2746
atmf recover led-off. 2747
atmf recover over-eth. 2748
atmf recover. 2744
atmf recovery-server. 2749
atmf remote-login 2751
atmf restricted-login. 2753
atmf retry guest-link 2755
atmf secure-mode certificate expire 2758
atmf secure-mode certificate expiry 2759
atmf secure-mode certificate renew 2760
atmf secure-mode enable-all. 2761
atmf secure-mode 2756
atmf select-area 2763
atmf topology-gui enable. 124
atmf topology-gui enable. 2764
atmf trustpoint 2765
atmf virtual-crosslink 2767
atmf virtual-link description. 2772
atmf virtual-link protection 2773
atmf virtual-link 2769
atmf working-set 2775
atmf-arealink 2684
atmf-link 2686
attribute 2364
auth auth-fail vlan 2166
auth critical. 2168
auth dhcp-framed-ip-lease. 2169
auth dynamic-vlan-creation. 2171
auth guest-vlan forward 2176
auth guest-vlan hw-forwarding 2178
auth guest-vlan. 2174
auth host-mode 2179
auth log 2181
auth max-supplicant. 2183

auth multi-vlan-session 2185
auth priority 2186
auth profile (global) 2188
auth profile (interface) 2189
auth radius send nas-identifier 2338
auth radius send service-type 2339
auth reauthentication 2190
auth roaming disconnected 2191
auth roaming enable 2193
auth supplicant-ip 2195
auth supplicant-mac 2197
auth timeout connect-timeout 2200
auth timeout quiet-period 2201
auth timeout reauth-period 2202
auth timeout server-timeout 2204
auth timeout supp-timeout 2206
auth two-step enable 2207
auth two-step order 2210
authentication 2366
auth-mac accounting 2212
auth-mac authentication 2213
auth-mac enable 2214
auth-mac method 2216
auth-mac password 2218
auth-mac reauth-relearning 2219
auth-mac static 2220
auth-mac username 2221
authorization commands 2318
authorization commands 2441
auth-web accounting 2222
auth-web authentication 2223
auth-web enable 2224
auth-web forward 2226
auth-web idle-timeout enable 2229
auth-web idle-timeout timeout 2230

auth-web max-auth-fail 2231
auth-web method 2233
auth-web-server blocking-mode 2234
auth-web-server dhcp ipaddress 2235
auth-web-server dhcp lease 2236
auth-web-server dhcp-wpad-option 2237
auth-web-server host-name 2238
auth-web-server intercept-port 2239
auth-web-server ipaddress 2240
auth-web-server login-url 2242
auth-web-server page language 2241
auth-web-server page logo 2243
auth-web-server page sub-title 2244
auth-web-server page success-message 2245
auth-web-server page title 2246
auth-web-server page welcome-message 2247
auth-web-server ping-poll enable 2248
auth-web-server ping-poll failcount 2249
auth-web-server ping-poll interval 2250
auth-web-server ping-poll reauth-timer-refresh 2251
auth-web-server ping-poll timeout 2252
auth-web-server port 2253
auth-web-server redirect-delay-time 2254
auth-web-server redirect-url 2255
auth-web-server session-keep 2256
auth-web-server ssl intercept-port 2258
auth-web-server ssl 2257
autoboot enable 134
auto-cost reference bandwidth (IPv6 OSPF) 1199
auto-cost reference bandwidth 1086
auto-summary (BGP only) 1284
backpressure 540
bandwidth 1088
bandwidth 1201
banner exec 240

banner login (SSH) 3177
banner login (system) 242
banner motd 244
bgp aggregate-nexthop-check 1286
bgp always-compare-med 1287
bgp bestpath as-path ignore 1289
bgp bestpath compare-confed-aspath 1290
bgp bestpath compare-routerid 1291
bgp bestpath med remove-recv-med 1294
bgp bestpath med remove-send-med 1295
bgp bestpath med 1292
bgp client-to-client reflection 1296
bgp cluster-id 1297
bgp confederation identifier 1299
bgp confederation peers 1300
bgp config-type 1302
bgp dampening 1304
bgp damp-peer-oscillation (BGP only) 1306
bgp default ipv4-unicast 1307
bgp default local-preference (BGP only) 1308
bgp deterministic-med 1309
bgp enforce-first-as 1311
bgp fast-external-failover 1312
bgp graceful-restart graceful-reset 1315
bgp graceful-restart 1313
bgp log-neighbor-changes 1316
bgp memory maxallocation 1318
bgp nexthop-trigger delay 1320
bgp nexthop-trigger enable 1321
bgp nexthop-trigger-count 1319
bgp rfc1771-path-select (BGP only) 1322
bgp rfc1771-strict (BGP only) 1323
bgp router-id 1324
bgp scan-time (BGP only) 1326
bgp update-delay 1327

boot config-file backup 137
boot config-file 135
boot system backup 139
boot system 138
bootfile 2929
bridge-group 2777
capability opaque 1089
capability restart 1090
cc interval 337
cc multicast 339
cc unicast 340
cd 140
cfm-sf-notify 2598
channel-group 762
circuit-failover 2532
cisco-metric-behavior (RIP) 992
class 2067
class-map 2068
clear (MEP Attribute) 341
clear aaa local user lockout 189
clear aaa local user lockout 2320
clear application-proxy threat-protection 2778
clear arp security statistics 2456
clear arp-cache 843
clear atmf links statistics 2781
clear atmf links virtual 2780
clear atmf links 2779
clear atmf recovery-file 2782
clear atmf secure-mode certificates 2783
clear atmf secure-mode statistics 2784
clear bgp (ASN) 1331
clear bgp (IPv4 or IPv6 address) 1329
clear bgp * 1328
clear bgp external 1332
clear bgp ipv6 (ASN) (BGP4+ only) 1337

clear bgp ipv6 (ipv6 address) (BGP4+ only) 1334
clear bgp ipv6 dampening (BGP4+ only)....1335
clear bgp ipv6 external (BGP4+ only) 1338
clear bgp ipv6 flap-statistics (BGP4+ only) 1336
clear bgp ipv6 peer-group (BGP4+ only)....1339
clear bgp peer-group 1333
clear counter ipv6 dhcp-client....2995
clear counter mrp....2644
clear ethernet cfm errorlog....342
clear exception log 385
clear fiber-monitoring interface 311
clear g8032 erp-instance statistics....2602
clear g8032 erp-instance....2600
clear gvrp statistics 815
clear ip bgp (ASN) (BGP only)....1344
clear ip bgp (IPv4) (BGP only)....1341
clear ip bgp * (BGP only) 1340
clear ip bgp dampening (BGP only)....1342
clear ip bgp external (BGP only) 1345
clear ip bgp flap-statistics (BGP only) 1343
clear ip bgp peer-group (BGP only)....1346
clear ip dhcp binding 2930
clear ip dhcp snooping binding 2457
clear ip dhcp snooping statistics 2458
clear ip dns forwarding cache 900
clear ip igmp group....1620
clear ip igmp interface 1621
clear ip igmp 1619
clear ip mroute pim sparse-mode 1757
clear ip mroute statistics 1718
clear ip mroute 1717
clear ip ospf process 1091
clear ip pim sparse-mode bsr rp-set *....1755
clear ip pim sparse-mode packet statistics....1756
clear ip prefix-list 1347

clear ip prefix-list 1999
clear ip rip route 993
clear ipv6 dhcp client 2996
clear ipv6 mld group 1683
clear ipv6 mld interface 1684
clear ipv6 mld 1682
clear ipv6 mroute pim sparse-mode 1814
clear ipv6 mroute pim 1813
clear ipv6 mroute statistics 1720
clear ipv6 mroute 1719
clear ipv6 neighbors 925
clear ipv6 ospf process 1202
clear ipv6 pim sparse-mode bsr rp-set * 1815
clear ipv6 rip route 1046
clear lacp counters 764
clear line console 190
clear line vty 191
clear lldp statistics 3089
clear lldp table 3090
clear log buffered 387
clear log external 388
clear log permanent 389
clear log 386
clear loop-protection action 542
clear loop-protection counters 543
clear mac address-table dynamic 544
clear mac address-table static 546
clear mep counter 343
clear mls qos interface policer-counters 2069
clear ping-poll 3270
clear port counter 547
clear port-security intrusion 548
clear power-inline counters interface 787
clear radius local-server statistics 2372
clear scada modbus tcp server connection 3313

clear scada modbus tcp server statistics 3314
clear spanning-tree detected protocols (RSTP and MSTP) 674
clear spanning-tree statistics 673
clear ssh 3178
clear test cable-diagnostics tdr 312
client (radsecproxy-srv) 2367
client mutual-authentication 2369
client name-check 2370
client trustpoint 2371
clock set 246
clock summer-time date 247
clock summer-time recurring 249
clock timezone 251
clock-port 3040
clone (amf-provision) 2785
commit (IPv4) 1936
commit (IPv6) 2017
compatible rfc1583 1092
configure boot config (amf-provision) 2787
configure boot system (amf-provision) 2789
configure terminal 113
continuous-reboot-prevention 252
copy (amf-provision) 2791
copy (filename) 141
copy buffered-log 390
copy debug 143
copy fdb-radius-users (to file) 2373
copy local-radius-user-db (from file) 2375
copy local-radius-user-db (to file) 2376
copy permanent-log 391
copy proxy-autoconfig-file 2259
copy running-config 144
copy startup-config 145
copy web-auth-https-file 2260
copy zmodem 146

create (amf-provision) 2792
create autoboot 147
critical-interval 3271
crypto key destroy hostkey 3179
crypto key destroy userkey 3180
crypto key generate hostkey 3181
crypto key generate rsa 2407
crypto key generate userkey 3183
crypto key pubkey-chain knownhosts 3184
crypto key pubkey-chain userkey 3186
crypto key zeroize 2408
crypto pki authenticate 2409
crypto pki enroll local (deleted) 2377
crypto pki enroll local local-radius-all-users (deleted) 2378
crypto pki enroll local user (deleted) 2379
crypto pki enroll user 2411
crypto pki enroll 2410
crypto pki export local pem (deleted) 2380
crypto pki export local pkcs12 (deleted) 2381
crypto pki export pem 2413
crypto pki export pkcs12 2414
crypto pki import pem 2416
crypto pki import pkcs12 2418
crypto pki trustpoint local (deleted) 2382
crypto pki trustpoint 2419
crypto secure-mode delete hostkey 2421
crypto secure-mode 2420
crypto secure-mode 254
crypto verify 148
crypto verify 2422
cut-through 550
data-traffic 2603
day 3232
deadtime (RADIUS server group) 2340
debug aaa 2321

debug alarm....533
debug arp security....2459
debug atmf packet....2796
debug atmf....2794
debug bgp (BGP only)....1348
debug core-file....255
debug crypto pki (deleted)....2383
debug dot1x....2131
debug epsr....2570
debug fiber-monitoring....313
debug g8032....2605
debug gvrp....816
debug igmp....1622
debug ip dhcp snooping....2460
debug ip dns forwarding....901
debug ip irdp....846
debug ip packet interface....844
debug ipv6 ospf events....1203
debug ipv6 ospf ifsm....1204
debug ipv6 ospf lsa....1205
debug ipv6 ospf nfsm....1206
debug ipv6 ospf packet....1207
debug ipv6 ospf route....1208
debug ipv6 pim sparse-mode packet....1818
debug ipv6 pim sparse-mode timer....1819
debug ipv6 pim sparse-mode....1816
debug ipv6 rip....1047
debug lacp....765
debug lldp....3091
debug loopprot....551
debug mail....3148
debug mld....1685
debug mrp....2645
debug mstp (RSTP and STP)....675
debug nsm mcast....1723

debug nsm mcast6 1724
debug nsm 1722
debug ospf events 1093
debug ospf ifsm 1094
debug ospf lsa 1095
debug ospf nfsm 1096
debug ospf nsm 1097
debug ospf packet 1098
debug ospf route 1099
debug pim dense-mode all 1875
debug pim dense-mode context 1876
debug pim dense-mode decode 1877
debug pim dense-mode encode 1878
debug pim dense-mode fsm 1879
debug pim dense-mode mrt 1880
debug pim dense-mode nexthop 1881
debug pim dense-mode nsm 1882
debug pim dense-mode vif 1883
debug pim sparse-mode timer 1759
debug pim sparse-mode 1758
debug ping-poll 3272
debug platform packet 552
debug power-inline 788
debug private-vlan ufo 613
debug radius 2341
debug rip 994
debug sflow agent 3294
debug sflow 3293
debug snmp 3049
debug ssh client 3188
debug ssh server 3189
debug trigger 3234
debug udld 746
debug vrrp events 2535
debug vrrp packet 2536

debug vrrp 2534
default log buffered 392
default log console 393
default log email 394
default log external 395
default log host 396
default log monitor 397
default log permanent 398
default-action 2070
default-information originate (IPv6 RIPng) 1048
default-information originate (RIP) 995
default-information originate 1100
default-information originate 1209
default-metric (IPv6 OSPF) 1210
default-metric (IPv6 RIPng) 1049
default-metric (OSPF) 1101
default-metric (RIP) 996
default-router 2931
delete (amf-provision) 2799
delete debug 151
delete mail 3149
delete 150
description (amf-container) 2803
description (auth-profile) 2261
description (interface) 480
description (ping-polling) 3273
description (QoS policy-map) 2071
description (trigger) 3235
dir 152
disable (Privileged Exec mode) 114
disable (VRRP) 2537
discovery 2801
distance (BGP and BGP4+) 1350
distance (IPv6 OSPF) 1211
distance (OSPF) 1102

distance (RIP) 997
distribute-list (IPv6 OSPF) 1213
distribute-list (IPv6 RIPng) 1050
distribute-list (OSPF) 1104
distribute-list (RIP) 998
dns-server 2932
do 115
domain-id (mrp-ring) 2646
domain-name (mrp-ring) 2647
domain-name 2933
domain-style 2384
dos 2000
dot1x accounting 2129
dot1x authentication 2130
dot1x control-direction 2132
dot1x eap 2134
dot1x eapol-version 2135
dot1x initialize interface 2136
dot1x initialize supplicant 2137
dot1x keytransmit 2138
dot1x max-auth-fail 2139
dot1x max-reauth-req 2141
dot1x port-control 2143
dot1x timeout tx-period 2145
duplex 554
echo 477
ecofriendly led 256
ecofriendly lpi 257
edit (filename) 155
edit 154
egress-rate-limit overhead 2074
egress-rate-limit 2072
egress-vlan-id 2385
egress-vlan-name 2387
enable (g8032-profile) 2606

enable (mrp-ring) 2648
enable (Privileged Exec mode) 116
enable (VRRP) 2538
enable db-summary-opt 1107
enable password 192
enable secret (deprecated) 195
end 118
enrollment (ca-trustpoint) 2424
epsr configuration 2572
epsr datavlan 2573
epsr enhancedrecovery enable 2574
epsr flush-type 2575
epsr mode master controlvlan primary port 2577
epsr mode transit controlvlan 2578
epsr priority 2579
epsr state 2580
epsr topology-change 2581
epsr topology-change 2607
epsr trap 2582
epsr 2571
erase factory-default 156
erase factory-default 2804
erase proxy-autoconfig-file 2262
erase startup-config 157
erase web-auth-https-file 2263
erp-instance 2608
ethernet cfm domain-name 344
ethernet cfm mep 347
exec-timeout 196
exit 119
exit-address-family 1352
fail-count 3274
fiber-monitoring action 315
fiber-monitoring baseline 317
fiber-monitoring enable 319

fiber-monitoring interval....320
fiber-monitoring sensitivity....321
findme trigger....261
findme....259
fingerprint (ca-trustpoint)....2425
flowcontrol (switch port)....555
flowcontrol hardware (asyn/console)....198
fullupdate (RIP)....999
g8032 erp-instance....2609
g8032 forced-switch erp-instance....2611
g8032 manual-switch erp-instance....2613
g8032 physical-ring....2614
g8032 profile....2616
group....2389
gvrp (interface)....818
gvrp dynamic-vlan-creation....819
gvrp enable (global)....820
gvrp registration....821
gvrp timer....822
help radius-attribute....2391
help....120
host (DHCP)....2934
host area....1108
hostname....262
http log webapi-requests....125
http port....126
http secure-port....127
http-enable....2805
identity (amf-provision)....2807
instance priority (MSTP)....679
instance vlan (MSTP)....681
interface (to configure)....481
ip (ip-host-group)....1937
ip (ping-polling)....3275
ip address (IP Addressing and Protocol)....847

ip address dhcp 2935
ip as-path access-list 1353
ip community-list expanded 1357
ip community-list standard 1359
ip community-list 1355
ip dhcp bootp ignore 2937
ip dhcp leasequery enable 2938
ip dhcp option 2939
ip dhcp pool 2941
ip dhcp snooping agent-option allow-untrusted 2464
ip dhcp snooping agent-option circuit-id vlantriplet 2465
ip dhcp snooping agent-option remote-id 2466
ip dhcp snooping agent-option 2463
ip dhcp snooping binding 2467
ip dhcp snooping database 2468
ip dhcp snooping delete-by-client 2469
ip dhcp snooping delete-by-linkdown 2470
ip dhcp snooping max-bindings 2471
ip dhcp snooping subscriber-id 2472
ip dhcp snooping trust 2473
ip dhcp snooping verify mac-address 2474
ip dhcp snooping violation 2475
ip dhcp snooping 2461
ip dhcp-client default-route distance 2942
ip dhcp-client request vendor-identifying-specific 2944
ip dhcp-client vendor-identifying-class 2945
ip dhcp-relay agent-option checking 2948
ip dhcp-relay agent-option checking 3000
ip dhcp-relay agent-option remote-id 2949
ip dhcp-relay agent-option remote-id 3001
ip dhcp-relay agent-option subscriber-id-auto-mac 2999
ip dhcp-relay agent-option 2946
ip dhcp-relay agent-option 2997
ip dhcp-relay information policy 2950
ip dhcp-relay information policy 3002

ip dhcp-relay maxhops 2952
ip dhcp-relay maxhops 3004
ip dhcp-relay max-message-length....2953
ip dhcp-relay max-message-length....3005
ip dhcp-relay server-address 2955
ip dhcp-relay server-address 3007
ip dhcp-relay use-client-side-address....2957
ip directed-broadcast....849
ip dns forwarding cache 903
ip dns forwarding dead-time....904
ip dns forwarding retry 905
ip dns forwarding source-interface 906
ip dns forwarding timeout 907
ip dns forwarding....902
ip domain-list....908
ip domain-lookup 909
ip domain-name....911
ip extcommunity-list expanded 1361
ip extcommunity-list standard 1363
ip forwarding....851
ip forward-protocol udp 852
ip gratuitous-arp-link 854
ip helper-address....856
ip icmp error-interval 859
ip igmp access-group....1624
ip igmp flood specific-query 1627
ip igmp flood-group....1625
ip igmp immediate-leave 1628
ip igmp last-member-query-count 1629
ip igmp last-member-query-interval....1630
ip igmp limit....1631
ip igmp maximum-groups 1632
ip igmp mroute-proxy 1634
ip igmp proxy-service....1635
ip igmp querier-timeout 1636

ip igmp query-holdtime 1637
ip igmp query-interval 1639
ip igmp query-max-response-time 1641
ip igmp ra-option....1643
ip igmp robustness-variable 1644
ip igmp snooping fast-leave....1646
ip igmp snooping mrouter 1647
ip igmp snooping querier 1648
ip igmp snooping report-suppression 1649
ip igmp snooping routermode 1650
ip igmp snooping source-timeout....1652
ip igmp snooping tcn query solicit 1653
ip igmp snooping....1645
ip igmp source-address-check 1655
ip igmp ssm 1656
ip igmp ssm-map enable....1657
ip igmp ssm-map static 1658
ip igmp startup-query-count....1662
ip igmp startup-query-interval 1663
ip igmp static-group 1660
ip igmp trusted 1664
ip igmp version....1665
ip igmp....1623
ip irdp address preference 860
ip irdp broadcast 861
ip irdp holdtime 862
ip irdp lifetime....863
ip irdp maxadvertinterval 864
ip irdp minadvertinterval 866
ip irdp multicast 868
ip irdp preference 869
ip irdp....858
ip limited-local-proxy-arp 870
ip local-proxy-arp....871
ip mroute 1725

ip multicast allow-register-fragments....1727
ip multicast allow-register-fragments....1761
ip multicast forward-first-packet....1728
ip multicast route....1729
ip multicast route-limit....1731
ip multicast wrong-vif-suppression....1732
ip multicast-routing....1733
ip name-server preferred-order....914
ip name-server....912
ip ospf authentication....1109
ip ospf authentication-key....1110
ip ospf cost....1111
ip ospf database-filter....1112
ip ospf dead-interval....1113
ip ospf disable all....1114
ip ospf hello-interval....1115
ip ospf message-digest-key....1116
ip ospf mtu....1118
ip ospf mtu-ignore....1119
ip ospf network....1120
ip ospf priority....1121
ip ospf resync-timeout....1122
ip ospf retransmit-interval....1123
ip ospf transmit-delay....1124
ip pim accept-register list....1762
ip pim anycast-rp....1763
ip pim bsr-border....1764
ip pim bsr-candidate....1765
ip pim cisco-register-checksum group-list....1767
ip pim cisco-register-checksum....1766
ip pim crp-cisco-prefix....1768
ip pim dense-mode passive....1885
ip pim dense-mode wrong-vif-suppression....1886
ip pim dense-mode....1884
ip pim dr-priority....1769

ip pim exclude-genid 1770
ip pim ext-srcs-directly-connected 1771
ip pim ext-srcs-directly-connected 1887
ip pim hello-holdtime (PIM-DM) 1888
ip pim hello-holdtime (PIM-SM) 1772
ip pim hello-interval (PIM-DM) 1889
ip pim hello-interval (PIM-SM) 1773
ip pim ignore-rp-set-priority 1774
ip pim jp-timer 1775
ip pim max-graft-retries 1890
ip pim neighbor-filter (PIM-DM) 1892
ip pim neighbor-filter (PIM-SM) 1776
ip pim propagation-delay 1893
ip pim register-rate-limit 1777
ip pim register-rp-reachability 1778
ip pim register-source 1779
ip pim register-suppression 1780
ip pim rp-address 1781
ip pim rp-candidate 1783
ip pim rp-register-kat 1785
ip pim sparse-mode join-prune-batching 1787
ip pim sparse-mode passive 1788
ip pim sparse-mode wrong-vif-suppression 1789
ip pim sparse-mode 1786
ip pim spt-threshold group-list 1791
ip pim spt-threshold 1790
ip pim ssm 1792
ip pim state-refresh origination-interval 1894
ip prefix-list 1001
ip prefix-list 1365
ip prefix-list 2003
ip proxy-arp 872
ip radius source-interface 2342
ip redirects 873
ip rip authentication key-chain 1003

ip rip authentication mode....1005
ip rip authentication string....1008
ip rip receive version....1011
ip rip receive-packet....1010
ip rip send version 1-compatible....1015
ip rip send version....1013
ip rip send-packet....1012
ip rip split-horizon....1017
ip route....971
ip source binding....2476
ip summary-address rip....1000
ip tacacs source-interface....2443
ip tcp synack-retries....874
ip tftp source-interface....158
ip unreachables....875
ipv6 (ipv6-host-group)....2018
ipv6 access-list (named IPv6 hardware ACL)....2020
ipv6 access-list extended (named)....2043
ipv6 access-list extended proto....2047
ipv6 access-list standard (named)....2055
ipv6 address autoconfig....928
ipv6 address dhcp....3009
ipv6 address suffix....930
ipv6 address....926
ipv6 enable....931
ipv6 eui64-linklocal....933
ipv6 forwarding....934
ipv6 icmp error-interval....935
ipv6 mld access-group....1687
ipv6 mld immediate-leave....1688
ipv6 mld last-member-query-count....1689
ipv6 mld last-member-query-interval....1690
ipv6 mld limit....1691
ipv6 mld querier-timeout....1693
ipv6 mld query-interval....1694

ipv6 mld query-max-response-time 1695
ipv6 mld robustness-variable 1696
ipv6 mld snooping fast-leave 1699
ipv6 mld snooping mrouter 1700
ipv6 mld snooping querier 1702
ipv6 mld snooping report-suppression 1703
ipv6 mld snooping 1697
ipv6 mld ssm-map enable 1705
ipv6 mld ssm-map static 1706
ipv6 mld static-group 1707
ipv6 mld version 1709
ipv6 mld 1686
ipv6 mroute 1734
ipv6 multicast forward-slow-path-packet 1721
ipv6 multicast forward-slow-path-packet 936
ipv6 multicast route 1736
ipv6 multicast route-limit 1739
ipv6 multicast-routing 1740
ipv6 nd accept-ra-default-routes 937
ipv6 nd accept-ra-pinfo 938
ipv6 nd current-hoplimit 939
ipv6 nd dns search-list 940
ipv6 nd dns-server 941
ipv6 nd managed-config-flag 942
ipv6 nd minimum-ra-interval 943
ipv6 nd other-config-flag 944
ipv6 nd prefix 945
ipv6 nd raguard 949
ipv6 nd ra-interval 947
ipv6 nd ra-lifetime 948
ipv6 nd reachable-time 951
ipv6 nd retransmission-time 952
ipv6 nd route-information 953
ipv6 nd router-preference 954
ipv6 nd suppress-ra 955

ipv6 neighbor 956
ipv6 opportunistic-nd 957
ipv6 ospf authentication spi 1215
ipv6 ospf cost 1217
ipv6 ospf dead-interval 1218
ipv6 ospf display route single-line 1219
ipv6 ospf encryption spi esp 1220
ipv6 ospf hello-interval 1223
ipv6 ospf neighbor 1224
ipv6 ospf network 1226
ipv6 ospf priority 1227
ipv6 ospf retransmit-interval 1228
ipv6 ospf transmit-delay 1229
ipv6 pim accept-register 1821
ipv6 pim anycast-rp 1822
ipv6 pim bsr-border 1823
ipv6 pim bsr-candidate 1824
ipv6 pim cisco-register-checksum group-list 1826
ipv6 pim cisco-register-checksum 1825
ipv6 pim crp-cisco-prefix 1827
ipv6 pim dr-priority 1828
ipv6 pim exclude-genid 1829
ipv6 pim ext-srcs-directly-connected 1830
ipv6 pim hello-holdtime 1831
ipv6 pim hello-interval 1832
ipv6 pim ignore-rp-set-priority 1833
ipv6 pim jp-timer 1834
ipv6 pim neighbor-filter 1835
ipv6 pim register-rate-limit 1836
ipv6 pim register-rp-reachability 1837
ipv6 pim register-source 1838
ipv6 pim register-suppression 1839
ipv6 pim rp embedded 1844
ipv6 pim rp-address 1840
ipv6 pim rp-candidate 1842

ipv6 pim rp-register-kat....1845
ipv6 pim sparse-mode passive....1847
ipv6 pim sparse-mode....1846
ipv6 pim spt-threshold group-list....1849
ipv6 pim spt-threshold....1848
ipv6 pim ssm....1850
ipv6 pim unicast-bsm....1851
ipv6 prefix-list....1051
ipv6 prefix-list....1367
ipv6 prefix-list....2059
ipv6 rip metric-offset....1053
ipv6 rip split-horizon....1055
ipv6 route....958
ipv6 route....973
ipv6 router ospf area....1230
ipv6 router rip....1056
ipv6 tftp source-interface....159
ipv6 traffic-filter....2022
ipv6 unreachables....959
key chain....1019
key....1018
key-string....1020
lacp global-passive-mode enable....766
lacp port-priority....767
lacp system-priority....768
lacp timeout....769
lc-react....2649
lease....2959
length (asyn)....200
length (ping-poll data)....3276
level (g8032-switch)....2617
license update file....235
license update online....236
license....228
license-cert (amf-provision)....2809

line....201
linkflap action....557
lldp faststart-count....3093
lldp holdtime-multiplier....3094
lldp management-address....3095
lldp med-notifications....3096
lldp med-tlv-select....3097
lldp non-strict-med-tlv-order-check....3100
lldp notification-interval....3101
lldp notifications....3102
lldp port-number-type....3103
lldp reinit....3104
lldp run....3105
lldp timer....3106
lldp tlv-select....3107
lldp transmit receive....3109
lldp tx-delay....3110
local-proxy-arp....877
locate (amf-provision)....2811
location civic-location configuration....3111
location civic-location identifier....3115
location civic-location-id....3116
location coord-location configuration....3117
location coord-location identifier....3119
location coord-location-id....3120
location elin-location....3122
location elin-location-id....3123
log buffered (filter)....400
log buffered exclude....403
log buffered size....406
log buffered....399
log console (filter)....408
log console exclude....411
log console....407
log email (filter)....415

log email exclude....418
log email time....421
log email....414
log event-host....128
log event-host....2813
log external (filter)....425
log external exclude....428
log external rotate....431
log external size....433
log external....423
log facility....434
log host (filter)....438
log host exclude....441
log host source....444
log host startup-delay....445
log host time....447
log host....436
log monitor (filter)....449
log monitor exclude....452
log permanent (filter)....456
log permanent exclude....459
log permanent size....462
log permanent....455
log trustpoint....464
login authentication....2322
login-fallback enable....2814
logout....121
log-rate-limit nsm....463
loop-protection action....559
loop-protection action-delay-time....560
loop-protection loop-detect....558
loop-protection timeout....561
mac address-table acquire....562
mac address-table ageing-time....563
mac address-table logging....564

mac address-table static 565
mac address-table thrash-limit 566
mail from....3152
mail smtpserver authentication 3154
mail smtpserver port....3156
mail smtpserver 3153
mail 3150
match access-group 2075
match as-path 1369
match as-path 1575
match community 1371
match community 1577
match cos 2077
match dscp....2078
match eth-format protocol....2079
match inner-cos 2082
match inner-vlan 2083
match interface....1579
match ip address 1580
match ip next-hop....1582
match ip-precedence 2084
match ipv6 address 1584
match ipv6 next-hop 1586
match mac-type 2085
match metric 1587
match origin....1588
match route-type....1590
match tag 1591
match tcp-flags....2086
match vlan 2087
max-concurrent-dd (IPv6 OSPF) 1232
max-concurrent-dd 1125
max-fib-routes....264
max-fib-routes....974
maximum-access-list (deleted) 2005

maximum-area 1126
maximum-paths 976
maximum-prefix 1021
max-paths 1373
max-static-routes 265
max-static-routes 975
mep (FNG attributes) 349
mep active 351
mep ccm-ltm-priority 353
mep crosscheck 355
mirror interface 496
mkdir 160
mls qos cos 2088
mls qos enable 2089
mls qos map cos-queue 2090
mls qos map premark-dscp 2091
modeltype 2815
move debug 162
move 161
mrp ring 2650
mru 483
mtu 484
multicast 1741
nas 2390
neighbor (IPv6 RIPng) 1057
neighbor (OSPF) 1127
neighbor (RIP) 1022
neighbor activate 1374
neighbor advertisement-interval 1377
neighbor allowas-in 1380
neighbor as-origination-interval 1383
neighbor attribute-unchanged 1385
neighbor capability graceful-restart 1388
neighbor capability orf prefix-list 1391
neighbor capability route-refresh 1394

neighbor collide-established 1397
neighbor default-originate 1400
neighbor description 1403
neighbor disallow-infinite-holdtime 1406
neighbor distribute-list 1408
neighbor dont-capability-negotiate 1411
neighbor ebgp-multihop 1414
neighbor enforce-multihop 1417
neighbor filter-list 1420
neighbor interface 1423
neighbor local-as 1424
neighbor maximum-prefix 1427
neighbor next-hop-self 1430
neighbor override-capability 1433
neighbor passive 1435
neighbor password 1438
neighbor peer-group (add a neighbor) 1441
neighbor peer-group (create a peer-group) 1443
neighbor port 1444
neighbor prefix-list 1447
neighbor remote-as 1450
neighbor remove-private-AS (BGP only) 1453
neighbor restart-time 1455
neighbor route-map 1458
neighbor route-reflector-client (BGP only) 1462
neighbor route-server-client (BGP only) 1464
neighbor send-community 1465
neighbor shutdown 1469
neighbor soft-reconfiguration inbound 1471
neighbor timers 1474
neighbor transparent-as 1477
neighbor transparent-nexthop 1479
neighbor unsuppress-map 1481
neighbor update-source 1484
neighbor version (BGP only) 1488

neighbor weight....1490
network (BGP and BGP4+)....1493
network (DHCP)....2961
network (RIP)....1023
network area....1128
network synchronization....1496
next-server....2962
no crypto pki certificate....2427
no debug all....266
no police....2093
normal-interval....3277
ntp authentication-key....3021
ntp broadcastdelay....3023
ntp master....3024
ntp peer....3025
ntp rate-limit....3027
ntp restrict....3028
ntp server....3030
ntp source....3032
offset-list (IPv6 RIPng)....1058
offset-list (RIP)....1024
openflow controller....2503
openflow datapath-id....2505
openflow failmode....2506
openflow inactivity....2508
openflow native vlan....2509
openflow ssl peer certificate....2510
openflow ssl trustpoint....2511
openflow version....2512
openflow....2502
optimistic-nd....878
optimistic-nd....960
option....2963
ospf abr-type....1130
ospf restart grace-period....1131

ospf restart helper 1132
ospf router-id....1134
overflow database external 1136
overflow database....1135
passive-interface (IPv6 OSPF)....1233
passive-interface (IPv6 RIPng) 1059
passive-interface (OSPF) 1137
passive-interface (RIP) 1025
physical-ring 2618
ping ipv6....961
ping....879
ping-poll 3278
platform hwfilter-size 567
platform l3-vlan-hashing-algorithm 2264
platform l3-vlan-hashing-algorithm 568
platform load-balancing 569
platform load-balancing 771
platform mac-vlan-hashing-algorithm....2265
platform mac-vlan-hashing-algorithm....570
platform multicast-ratelimit....1742
platform multicast-ratelimit....571
platform stop-unreg-mc-flooding 572
platform vlan-stacking-tpid 574
platform vlan-stacking-tpid 614
polarity....575
police single-rate action 2094
police twin-rate action....2096
policy-map 2098
port-vlan-forwarding-priority 615
power-inline allow-legacy....790
power-inline description....791
power-inline enable 792
power-inline hanp....793
power-inline max....794
power-inline priority....796

power-inline usage-threshold 798
power-inline wattage max 799
preempt-mode 2539
priority 2541
priority-queue 2099
private-vlan association 620
private-vlan ufo trap 621
private-vlan 618
privilege level 203
probe enable 2965
probe packets 2966
probe timeout 2967
probe type 2968
profile (mrp-ring) 2652
profile name 2619
proxy-port 2323
ptp global 3043
ptp-clk 3041
pwd 163
radius-secure-proxy aaa 2324
radius-secure-proxy local-server 2393
radius-server deadtime 2343
radius-server host 2344
radius-server key 2348
radius-server local 2394
radius-server retransmit 2350
radius-server timeout 2352
range 2969
raps-channel 2620
reboot 268
recv-buffer-size (IPv6 RIPng) 1060
recv-buffer-size (RIP) 1026
redistribute (into BGP or BGP4+) 1497
redistribute (IPv6 OSPF) 1234
redistribute (IPv6 RIPng) 1061

redistribute (OSPF) 1138
redistribute (RIP) 1027
region (MSTP) 683
reload 269
remark new-cos 2102
remark-map 2100
remote-mirror interface 498
repeat 3236
restart bgp graceful (BGP only) 1499
restart ipv6 ospf graceful 1236
restart ospf graceful 1140
restart rip graceful 1028
revision (MSTP) 684
rip restart grace-period 1029
rmdir 164
rmon alarm 3162
rmon collection history 3165
rmon collection stats 3166
rmon event 3167
role (mrp-ring) 2653
route (IPv6 RIPng) 1062
route (RIP) 1030
route 2970
route-map 1501
route-map 1592
router bgp 1500
router ip irdp 880
router ipv6 ospf 1237
router ipv6 rip 1063
router ipv6 vrrp (interface) 2543
router ospf 1141
router rip 1031
router vrrp (interface) 2545
router-id (IPv6 OSPF) 1238
router-id 1142

rpl role 2622
rsakeypair (ca-trustpoint) 2428
sample-size 3279
scada modbus tcp server access permit 3316
scada modbus tcp server access 3315
scada modbus tcp server connection 3317
scada modbus tcp server port 3318
scada modbus tcp server 3319
script 3237
security-password forced-change 205
security-password history 204
security-password lifetime 206
security-password minimum-categories 208
security-password minimum-length 209
security-password min-lifetime-enforce 207
security-password reject-expired-pwd 210
security-password warning 211
send-lifetime 1032
server (radsecproxy-aaa) 2325
server (server group) 2354
server auth-port 2395
server enable 2396
server mutual-authentication 2327
server name-check 2328
server trustpoint 2329
service advanced-vty 212
service atmf-application-proxy 2816
service dhcp-relay 2971
service dhcp-relay 3011
service dhcp-server 2972
service dhcp-snooping 2478
service http 129
service ma-name 357
service mrp 2654
service onm 2621

service password-encryption....213
service pdm....1895
service pim....1793
service pim6....1852
service power-inline....800
service ssh....3190
service statistics interfaces counter....485
service telnet....214
service-policy input....2104
set aggregator....1595
set as-path....1504
set as-path....1596
set atomic-aggregate....1597
set comm-list delete....1598
set community....1505
set community....1599
set dampening....1601
set extcommunity....1603
set ip next-hop (route map)....1605
set ipv6 next-hop....1606
set local-preference....1607
set metric....1608
set metric-type....1610
set origin....1611
set originator-id....1612
set tag....1613
set weight....1614
sflow agent....3295
sflow collector max-datagram-size....3299
sflow collector....3297
sflow enable....3300
sflow max-header-size....3301
sflow polling-interval....3303
sflow sampling-rate....3304
short-lease-threshold....2973

show aaa local user locked 215
show aaa local user locked 2331
show aaa server group 2332
show access-group 1959
show access-list (IPv4 Hardware ACLs) 1960
show access-list (IPv4 Software ACLs) 2006
show acl-group ip address 1962
show acl-group ip port 1963
show acl-group ipv6 address 2039
show alarm facility settings 534
show alarm facility status 535
show application-proxy threat-protection 2817
show application-proxy whitelist advertised-address 2819
show application-proxy whitelist interface 2820
show application-proxy whitelist server 2822
show application-proxy whitelist supplicant 2823
show arp security interface 2481
show arp security statistics 2483
show arp security 2480
show arp 881
show atmf area guests 2832
show atmf area guests-detail 2834
show atmf area nodes 2836
show atmf area nodes-detail 2838
show atmf area summary 2840
show atmf area 2829
show atmf authorization 2841
show atmf backup area 2848
show atmf backup guest 2850
show atmf backup 2844
show atmf container 2852
show atmf detail 2855
show atmf group members 2859
show atmf group 2857
show atmf guests detail 2863

show atmf guests....2861
show atmf links detail....2868
show atmf links guest detail....2879
show atmf links guest....2877
show atmf links statistics....2883
show atmf links....2866
show atmf nodes....2886
show atmf provision nodes....2888
show atmf recovery-file....2890
show atmf secure-mode audit link....2894
show atmf secure-mode audit....2893
show atmf secure-mode certificates....2895
show atmf secure-mode sa....2898
show atmf secure-mode statistics....2901
show atmf secure-mode....2891
show atmf tech....2903
show atmf virtual-links....2906
show atmf working-set....2908
show atmf....2825
show auth diagnostics....2268
show auth interface....2270
show auth sessionstatistics....2272
show auth statistics interface....2273
show auth supplicant interface....2277
show auth supplicant....2274
show auth two-step supplicant brief....2278
show auth....2266
show auth-web-server page....2281
show auth-web-server....2280
show autoboot....165
show banner login....3192
show bgp ipv6 (BGP4+ only)....1507
show bgp ipv6 community (BGP4+ only)....1508
show bgp ipv6 community-list (BGP4+ only)....1510
show bgp ipv6 dampening (BGP4+ only)....1511

show bgp ipv6 filter-list (BGP4+ only) 1512
show bgp ipv6 inconsistent-as (BGP4+ only)....1513
show bgp ipv6 longer-prefixes (BGP4+ only)....1514
show bgp ipv6 neighbors (BGP4+ only) 1515
show bgp ipv6 paths (BGP4+ only) 1518
show bgp ipv6 prefix-list (BGP4+ only) 1519
show bgp ipv6 quote-regexp (BGP4+ only) 1520
show bgp ipv6 regexp (BGP4+ only)....1521
show bgp ipv6 route-map (BGP4+ only) 1523
show bgp ipv6 summary (BGP4+ only) 1524
show bgp memory maxallocation (BGP only) 1525
show bgp nexthop-tracking (BGP only)....1526
show bgp nexthop-tree-details (BGP only)....1527
show boot....166
show class-map 2105
show clock 270
show continuous-reboot-prevention 272
show counter dhcp-client....2975
show counter dhcp-relay 2976
show counter dhcp-relay 3012
show counter dhcp-server 2979
show counter ipv6 dhcp-client....3015
show counter log....465
show counter mail....3158
show counter mrp 2655
show counter ping-poll 3281
show counter snmp-server....3050
show cpu history 276
show cpu....273
show crypto key hostkey....3193
show crypto key mypubkey rsa....2429
show crypto key pubkey-chain knownhosts 3195
show crypto key pubkey-chain userkey....3196
show crypto key userkey....3197
show crypto pki certificates 2430

show crypto pki enrollment user 2432
show crypto pki trustpoint 2433
show debugging aaa 2333
show debugging alarm 536
show debugging arp security 2485
show debugging atmf packet 2910
show debugging atmf 2909
show debugging bgp (BGP only) 1528
show debugging dot1x 2147
show debugging epsr 2583
show debugging g8032 2624
show debugging gvrp 824
show debugging igmp 1666
show debugging ip dhcp snooping 2486
show debugging ip dns forwarding 915
show debugging ip packet 882
show debugging ipv6 ospf 1239
show debugging ipv6 pim sparse-mode 1853
show debugging ipv6 rip 1064
show debugging lacp 772
show debugging lldp 3124
show debugging loopprot 576
show debugging mld 1710
show debugging mrp 2659
show debugging mstp 685
show debugging nsm mcast 1743
show debugging ospf 1143
show debugging pim dense-mode 1896
show debugging pim sparse-mode 1794
show debugging platform packet 577
show debugging power-inline 801
show debugging private-vlan 622
show debugging radius 2356
show debugging rip 1034
show debugging sflow 3305

show debugging snmp 3054
show debugging trigger 3239
show debugging udld 747
show debugging vrrp 2547
show debugging 278
show dhcp lease 2981
show diagnostic channel-group 773
show dos interface 2008
show dot1x diagnostics 2151
show dot1x interface 2153
show dot1x sessionstatistics 2155
show dot1x statistics interface 2156
show dot1x supplicant interface 2159
show dot1x supplicant 2157
show dot1x 2148
show ecofriendly 279
show epsr <epsr-instance> counters 2592
show epsr <epsr-instance> 2591
show epsr common segments 2589
show epsr config-check 2590
show epsr counters 2593
show epsr summary 2594
show epsr 2584
show etherchannel detail 776
show etherchannel summary 777
show etherchannel 775
show ethernet cfm details 360
show ethernet cfm domain 365
show ethernet cfm errorlog 368
show ethernet cfm maintenance-points local mep 370
show ethernet cfm maintenance-points remote mep 376
show ethernet cfm service 379
show exception log 466
show file systems 169
show file 168

show flowcontrol interface 578
show g8032 erp-instance statistics 2630
show g8032 erp-instance 2625
show g8032 physical-ring 2632
show g8032 profile 2634
show gvrp configuration 825
show gvrp machine 826
show gvrp statistics 827
show gvrp timer 828
show history 122
show hosts 916
show http 130
show interface access-group 1964
show interface brief 489
show interface err-disabled 579
show interface memory 281
show interface memory 490
show interface status 492
show interface switchport vlan translation 623
show interface switchport 580
show interface 486
show ip access-list 2011
show ip bgp (BGP only) 1529
show ip bgp attribute-info (BGP only) 1530
show ip bgp cidr-only (BGP only) 1531
show ip bgp community (BGP only) 1532
show ip bgp community-info (BGP only) 1534
show ip bgp community-list (BGP only) 1535
show ip bgp dampening (BGP only) 1536
show ip bgp filter-list (BGP only) 1538
show ip bgp inconsistent-as (BGP only) 1539
show ip bgp longer-prefixes (BGP only) 1540
show ip bgp neighbors (BGP only) 1541
show ip bgp neighbors connection-retrytime (BGP only) 1544
show ip bgp neighbors hold-time (BGP only) 1545

show ip bgp neighbors keepalive (BGP only) 1546
show ip bgp neighbors keepalive-interval (BGP only) 1547
show ip bgp neighbors notification (BGP only).....1548
show ip bgp neighbors open (BGP only).....1549
show ip bgp neighbors rcvd-msgs (BGP only).....1550
show ip bgp neighbors sent-msgs (BGP only).....1551
show ip bgp neighbors update (BGP only).....1552
show ip bgp paths (BGP only) 1553
show ip bgp prefix-list (BGP only) 1554
show ip bgp quote-regexp (BGP only) 1555
show ip bgp regexp (BGP only).....1557
show ip bgp route-map (BGP only) 1559
show ip bgp scan (BGP only) 1560
show ip bgp summary (BGP only) 1561
show ip community-list.....1562
show ip dhcp binding.....2982
show ip dhcp pool.....2983
show ip dhcp server statistics 2989
show ip dhcp server summary 2991
show ip dhcp snooping acl.....2488
show ip dhcp snooping agent-option 2491
show ip dhcp snooping binding.....2493
show ip dhcp snooping interface.....2495
show ip dhcp snooping statistics.....2497
show ip dhcp snooping.....2487
show ip dhcp-relay 2988
show ip dhcp-relay 3017
show ip dns forwarding cache 918
show ip dns forwarding server 919
show ip dns forwarding.....917
show ip domain-list.....920
show ip domain-name.....921
show ip extcommunity-list.....1563
show ip flooding-nexthops 883
show ip forwarding.....884

show ip igmp groups 1667
show ip igmp interface 1669
show ip igmp proxy groups 1672
show ip igmp proxy 1671
show ip igmp snooping mrouter 1674
show ip igmp snooping routermode 1675
show ip igmp snooping source-timeout 1676
show ip igmp snooping statistics 1677
show ip interface 885
show ip irdp interface 887
show ip irdp 886
show ip mroute 1744
show ip mvif 1747
show ip name-server 922
show ip ospf border-routers 1147
show ip ospf database asbr-summary 1150
show ip ospf database external 1151
show ip ospf database network 1153
show ip ospf database nssa-external 1154
show ip ospf database opaque-area 1156
show ip ospf database opaque-as 1157
show ip ospf database opaque-link 1158
show ip ospf database router 1159
show ip ospf database summary 1161
show ip ospf database 1148
show ip ospf interface 1164
show ip ospf neighbor 1165
show ip ospf route 1167
show ip ospf virtual-links 1168
show ip ospf 1144
show ip pim dense-mode interface detail 1899
show ip pim dense-mode interface 1897
show ip pim dense-mode mroute 1900
show ip pim dense-mode neighbor detail 1902
show ip pim dense-mode neighbor 1901

show ip pim dense-mode nexthop 1903
show ip pim sparse-mode bsr-router 1795
show ip pim sparse-mode interface detail 1798
show ip pim sparse-mode interface 1796
show ip pim sparse-mode local-members 1799
show ip pim sparse-mode mroute detail 1802
show ip pim sparse-mode mroute 1800
show ip pim sparse-mode neighbor 1804
show ip pim sparse-mode nexthop 1805
show ip pim sparse-mode packet statistics 1806
show ip pim sparse-mode rp mapping 1808
show ip pim sparse-mode rp-hash 1807
show ip prefix-list 1035
show ip prefix-list 1564
show ip prefix-list 2012
show ip protocols bgp (BGP only) 1566
show ip protocols ospf 1169
show ip protocols rip 1036
show ip rip database 1038
show ip rip interface 1039
show ip rip 1037
show ip route database 980
show ip route summary 982
show ip route 977
show ip rpf 1748
show ip sockets 889
show ip source binding 2500
show ip traffic 892
show ipv6 access-list (IPv6 Hardware ACLs) 2040
show ipv6 access-list (IPv6 Software ACLs) 2061
show ipv6 dhcp interface 3019
show ipv6 dhcp 3018
show ipv6 forwarding 963
show ipv6 interface 964
show ipv6 mif 1752

show ipv6 mld groups 1711
show ipv6 mld interface 1712
show ipv6 mld snooping mrouter 1713
show ipv6 mld snooping statistics 1714
show ipv6 mroute 1749
show ipv6 multicast forwarding 1751
show ipv6 neighbors 965
show ipv6 ospf database external 1244
show ipv6 ospf database grace 1245
show ipv6 ospf database inter-prefix 1246
show ipv6 ospf database inter-router 1247
show ipv6 ospf database intra-prefix 1248
show ipv6 ospf database link 1249
show ipv6 ospf database network 1250
show ipv6 ospf database router 1252
show ipv6 ospf database 1242
show ipv6 ospf interface 1257
show ipv6 ospf neighbor 1259
show ipv6 ospf route 1261
show ipv6 ospf virtual-links 1263
show ipv6 ospf 1240
show ipv6 pim sparse-mode bsr-router 1854
show ipv6 pim sparse-mode interface detail 1857
show ipv6 pim sparse-mode interface 1855
show ipv6 pim sparse-mode local-members 1858
show ipv6 pim sparse-mode mroute detail 1862
show ipv6 pim sparse-mode mroute 1860
show ipv6 pim sparse-mode neighbor 1864
show ipv6 pim sparse-mode nexthop 1865
show ipv6 pim sparse-mode rp mapping 1867
show ipv6 pim sparse-mode rp nexthop 1868
show ipv6 pim sparse-mode rp-hash 1866
show ipv6 prefix-list 1065
show ipv6 prefix-list 1565
show ipv6 prefix-list 2063

show ipv6 protocols rip 1066
show ipv6 rip database 1068
show ipv6 rip interface 1069
show ipv6 rip 1067
show ipv6 route summary 968
show ipv6 route summary 985
show ipv6 route 966
show ipv6 route 983
show lacp sys-id 778
show lacp-counter 779
show license brief 232
show license external 237
show license 230
show lldp interface 3128
show lldp local-info 3130
show lldp neighbors detail 3137
show lldp neighbors 3135
show lldp statistics interface 3143
show lldp statistics 3141
show lldp 3126
show location 3145
show log config 469
show log external 471
show log permanent 472
show log 467
show loop-protection 581
show mac address-table thrash-limit 585
show mac address-table 583
show mail 3159
show memory allocations 285
show memory history 287
show memory pools 288
show memory shared 289
show memory 283
show mep-alarm status 382

show mirror interface 501
show mirror 500
show mls qos interface policer-counters 2110
show mls qos interface queue-counters 2111
show mls qos interface storm-status 2112
show mls qos interface 2107
show mls qos maps cos-queue 2113
show mls qos maps premark-dscp 2114
show mls qos 2106
show mrp ports 2660
show mrp ring 2661
show ntp associations 3034
show ntp counters associations 3037
show ntp counters 3036
show ntp status 3038
show openflow config 2513
show openflow coverage 2515
show openflow flows 2517
show openflow rules 2520
show openflow ssl 2522
show openflow status 2523
show ping-poll 3283
show platform classifier statistics utilization brief 2115
show platform classifier statistics utilization brief 589
show platform port 591
show platform 586
show policy-map 2117
show port etherchannel 780
show port-security interface 593
show port-security intrusion 594
show port-vlan-forwarding-priority 625
show power-inline counters 806
show power-inline interface detail 811
show power-inline interface 808
show power-inline 802

show privilege....216
show process....290
show proxy-autoconfig-file....2282
show ptp data transparent....3044
show ptp port....3045
show radius local-server group....2397
show radius local-server nas....2398
show radius local-server statistics....2399
show radius local-server user....2400
show radius server group....2334
show radius statistics....2360
show radius....2357
show reboot history....292
show remote-mirror....502
show rmon alarm....3168
show rmon event....3169
show rmon history....3171
show rmon statistics....3173
show route-map....1567
show route-map....1615
show router-id....293
show running-config atmf....2911
show running-config interface....174
show running-config log....473
show running-config router ipv6 vrrp....2548
show running-config router vrrp....2549
show running-config sflow....3307
show running-config snmp....3055
show running-config ssh....3198
show running-config trigger....3240
show running-config....171
show scada modbus tcp server connections....3320
show scada modbus tcp server....3322
show secure-mode....2434
show secure-mode....294

show security-password configuration 217
show security-password user 218
show sflow interface 3310
show sflow 3308
show snmp-server community 3057
show snmp-server group 3058
show snmp-server user 3059
show snmp-server view 3060
show snmp-server 3056
show spanning-tree brief 689
show spanning-tree mst config 691
show spanning-tree mst detail interface 694
show spanning-tree mst detail 692
show spanning-tree mst instance interface 697
show spanning-tree mst instance 696
show spanning-tree mst interface 698
show spanning-tree mst 690
show spanning-tree statistics instance interface 702
show spanning-tree statistics instance 701
show spanning-tree statistics interface 704
show spanning-tree statistics 699
show spanning-tree vlan range-index 706
show spanning-tree 686
show ssh client 3202
show ssh server allow-users 3205
show ssh server deny-users 3206
show ssh server 3203
show ssh 3200
show startup-config 177
show static-channel-group 781
show storm-control 595
show system environment counters 297
show system environment 296
show system fiber-monitoring 323
show system interrupts 299

show system mac....300
show system pci device....301
show system pci tree....302
show system pluggable detail....328
show system pluggable diagnostics....331
show system pluggable....326
show system serialnumber....303
show system....295
show tacacs+....2444
show tech-support....304
show telnet....219
show test cable-diagnostics tdr....333
show trigger....3241
show udld neighbors....749
show udld port....750
show udld....748
show users....220
show version....178
show vlan access-map....627
show vlan classifier group interface....629
show vlan classifier group....628
show vlan classifier interface group....630
show vlan classifier rule....631
show vlan filter....632
show vlan private-vlan ufo....634
show vlan private-vlan....633
show vlan....626
show vrrp (session)....2556
show vrrp counters....2552
show vrrp ipv6....2555
show vrrp....2550
shutdown....494
snmp trap link-status suppress....3062
snmp trap link-status....3061
snmp-server community....3066

snmp-server contact 3067
snmp-server enable trap 3068
snmp-server engineID local reset 3073
snmp-server engineID local 3071
snmp-server group 3074
snmp-server host 3076
snmp-server legacy-ifadminstatus 3078
snmp-server location 3079
snmp-server source-interface 3080
snmp-server startup-trap-delay 3081
snmp-server user 3082
snmp-server view 3085
snmp-server 3064
source-ip 3287
spanning-tree autoedge (RSTP and MSTP) 707
spanning-tree bpdu 708
spanning-tree cisco-interoperability (MSTP) 710
spanning-tree edgeport (RSTP and MSTP) 711
spanning-tree enable 712
spanning-tree errdisable-timeout enable 714
spanning-tree errdisable-timeout interval 715
spanning-tree force-version 716
spanning-tree forward-time 717
spanning-tree guard root 718
spanning-tree hello-time 719
spanning-tree link-type 720
spanning-tree max-age 721
spanning-tree max-hops (MSTP) 722
spanning-tree mode 723
spanning-tree mst configuration 724
spanning-tree mst instance path-cost 726
spanning-tree mst instance priority 728
spanning-tree mst instance restricted-role 729
spanning-tree mst instance restricted-tcn 731
spanning-tree mst instance 725

spanning-tree path-cost 732
spanning-tree portfast (STP) 733
spanning-tree portfast bpdu-filter 735
spanning-tree portfast bpdu-guard 737
spanning-tree priority (bridge priority) 739
spanning-tree priority (port priority) 740
spanning-tree restricted-role 741
spanning-tree restricted-tcn 742
spanning-tree transmit-holdcount 743
speed (asyn) 306
speed 596
ssh client 3210
ssh server allow-users 3214
ssh server authentication 3216
ssh server deny-users 3218
ssh server max-auth-tries 3220
ssh server resolve-host 3221
ssh server scp 3222
ssh server secure-ciphers 3223
ssh server secure-kex 3224
ssh server sftp 3226
ssh server 3212
ssh 3207
state 2912
static-channel-group 782
storm-action 2118
storm-control level 598
storm-downtime 2119
storm-protection 2120
storm-rate 2121
storm-window 2122
subject-name (ca-trustpoint) 2435
subnet-mask 2992
sub-ring 2636
summary-address (IPv6 OSPF) 1264

summary-address 1170
switchport access vlan 635
switchport atmf-agentlink 2914
switchport atmf-arealink 2915
switchport atmf-crosslink 2917
switchport atmf-guestlink 2919
switchport atmf-link 2921
switchport enable vlan 636
switchport mode access 637
switchport mode private-vlan trunk promiscuous 639
switchport mode private-vlan trunk secondary 641
switchport mode private-vlan ufo 643
switchport mode private-vlan 638
switchport mode trunk 645
switchport port-security aging 601
switchport port-security maximum 603
switchport port-security violation 605
switchport port-security 599
switchport private-vlan host-association 646
switchport private-vlan mapping 647
switchport remote-mirror-egress 504
switchport trunk allowed vlan 648
switchport trunk native vlan 651
switchport vlan translation default drop 654
switchport vlan translation 652
switchport vlan-stacking (double-tagging) 655
switchport voice dscp 656
switchport voice vlan priority 659
switchport voice vlan 657
synchronization 1568
tacacs-server host 2446
tacacs-server key 2448
tacacs-server timeout 2449
tcpdump 894
telnet server 222

telnet 221
terminal length 223
terminal monitor 308
terminal resize 224
test cable-diagnostics tdr interface 334
test 3246
thrash-limiting 607
time (trigger) 3247
timeout (ping polling) 3289
timer (g8032-profile) 2637
timers (BGP) 1570
timers (IPv6 RIPng) 1070
timers (RIP) 1040
timers spf exp (IPv6 OSPF) 1266
timers spf exp 1171
topology-change 2639
traceroute ipv6 969
traceroute 895
transition-mode 2558
trap (g8032-switch) 2641
trap 3249
trigger activate 3251
trigger 3250
trust dscp 2123
type atmf node 2922
type atmf node 3252
type cpu 3255
type interface 3256
type linkmon-probe 3257
type log 3259
type memory 3260
type periodic 3261
type ping-poll 3262
type reboot 3263
type time 3264

type usb....3265
udld aggressive-mode....751
udld enable....752
udld port aggressive-mode....754
udld port disable....755
udld port....753
udld reset....756
udld time disable-period....757
udld time message-interval....758
undebug aaa....2336
undebug all ipv6 pim sparse-mode....1870
undebug all pim dense-mode....1904
undebug all pim sparse-mode....1809
undebug all....309
undebug atmf....2925
undebug bgp (BGP only)....1572
undebug dot1x....2161
undebug epsr....2595
undebug g8032....2642
undebug igmp....1679
undebug ip irdp....897
undebug ip packet interface....896
undebug ipv6 ospf events....1267
undebug ipv6 ospf ifsm....1268
undebug ipv6 ospf lsa....1269
undebug ipv6 ospf nfsm....1270
undebug ipv6 ospf packet....1271
undebug ipv6 ospf route....1272
undebug ipv6 pim sparse-mode....1871
undebug ipv6 rip....1071
undebug lacp....784
undebug loopprot....609
undebug mail....3160
undebug mstp....744
undebug ospf events....1172

undebug ospf ifsm....1173
undebug ospf lsa....1174
undebug ospf nfsm....1175
undebug ospf nsm....1176
undebug ospf packet....1177
undebug ospf route....1178
undebug ping-poll....3291
undebug platform packet....610
undebug radius....2361
undebug rip....1041
undebug sflow....3311
undebug snmp....3086
undebug ssh client....3227
undebug ssh server....3228
undebug trigger....3266
undebug udld....759
undebug vrrp events....2561
undebug vrrp packet....2562
undebug vrrp....2560
unmount....179
unmount....474
up-count....3290
user (RADIUS server)....2402
username....225
username....2926
version (RIP)....1042
virtual-ip....2563
virtual-ipv6....2565
vlan (RADIUS server)....2404
vlan access-map....662
vlan classifier activate....663
vlan classifier group....664
vlan classifier rule ipv4....665
vlan classifier rule proto....666
vlan database....669

vlan filter 670
vlan mode remote-mirror-vlan 505
vlan 660
vlan-id (mrp-ring) 2663
vrrp vmac 2567
vty access-class (numbered) 2013
vty ipv6 access-class (named) 2064
wait 478
write file 180
write memory 181
write terminal 182
wrr-queue disable queues 2124
wrr-queue egress-rate-limit queues 2125
wrr-queue weight queues 2126

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 113
- "disable (Privileged Exec mode)" on page 114
- "do" on page 115
- "enable (Privileged Exec mode)" on page 116
- "end" on page 118
- "exit" on page 119
- "help" on page 120
- "logout" on page 121
- "show history" on page 122

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 vlan2
awplus(config-if)# end
awplus#
```

Related commands

disable (Privileged Exec mode)

enable (Privileged Exec mode)

exit

exit

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

Syntax

```
exit
```

Mode All command modes, including 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 vlan2
awplus(config-if)# exit
awplus(config)#
```

Related commands

disable (Privileged Exec mode)

enable (Privileged Exec mode)

end

help

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

Syntax `help`

Mode All command modes

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

```
awplus# help
```

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

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

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

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

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

logout

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

Syntax

```
logout
```

Mode User Exec and Privileged Exec

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

```
awplus# logout
```

show history

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

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

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

Syntax

```
show history
```

Mode User Exec and Privileged Exec

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

```
awplus# show history
```

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

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

2 Device GUI and Vista Manager EX Commands

Introduction

Overview

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

For more information, see Getting Started with the Device GUI on Switches.

Command List

- "atmf topology-gui enable" on page 124
- "http log webapi-requests" on page 125
- "http port" on page 126
- "http secure-port" on page 127
- "log event-host" on page 128
- "service http" on page 129
- "show http" on page 130

atmf topology-gui enable

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

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

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

Syntax

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

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

Mode Global Configuration mode

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

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

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

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

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

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

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

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

Related commands atmf enable

log event-host

service http

http log webapi-requests

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

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

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

Syntax

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

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

Default Web API request logging is disabled.

Mode Global Configuration

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

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

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

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

Related commands

http port

service http

show log

Command changes Version 5.4.8-1.1: command added

http port

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

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

Syntax

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

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

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

Mode Global Configuration

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

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

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

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

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

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

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

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

Related commands http secure-port

service http

show http

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

Version 5.4.8-0.2: command added on AlliedWare Plus switches

http secure-port

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

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

Syntax

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

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

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

Mode Global Configuration

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

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

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

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

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

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

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

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

Related commands http port

service http

show http

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

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

Version 5.4.8-0.2: command added on AlliedWare Plus switches

log event-host

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

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

Syntax

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

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

Default Log events are disabled by default.

Mode Global Configuration

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

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

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

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

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

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

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

Related commands atmf topology-gui enable

service http

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

This service is required to support Vista Manager EX™ and the Device GUI.

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

Syntax

```
service http
no service http
```

Default Enabled

Mode Global Configuration

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

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

To disable the HTTP service, use the following commands:

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

Related commands

http port

http secure-port

show http

show http

Overview This command shows the HTTP server settings.

Syntax

```
show http
```

Mode User Exec and Privileged Exec

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

```
awplus# show http
```

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

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

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 to or from a USB storage device	`usb:[/][<directory>/]<filename>`	To specify a file in the top-level directory of the USB stick: usb: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:/`

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

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

Command List

- "autoboot enable" on page 134
- "boot config-file" on page 135
- "boot config-file backup" on page 137
- "boot system" on page 138

- "boot system backup" on page 139
- "cd" on page 140
- "copy (filename)" on page 141
- "copy debug" on page 143
- "copy running-config" on page 144
- "copy startup-config" on page 145
- "copy zmodem" on page 146
- "create autoboot" on page 147
- "crypto verify" on page 148
- "delete" on page 150
- "delete debug" on page 151
- "dir" on page 152
- "edit" on page 154
- "edit (filename)" on page 155
- "erase factory-default" on page 156
- "erase startup-config" on page 157
- "ip tftp source-interface" on page 158
- "ipv6 tftp source-interface" on page 159
- "mkdir" on page 160
- "move" on page 161
- "move debug" on page 162
- "pwd" on page 163
- "rmdir" on page 164
- "show autoboot" on page 165
- "show boot" on page 166
- "show file" on page 168
- "show file systems" on page 169
- "show running-config" on page 171
- "show running-config interface" on page 174
- "show startup-config" on page 177
- "show version" on page 178
- "unmount" on page 179
- "write file" on page 180
- "write memory" on page 181
- "write terminal" on page 182

autoboot enable

Overview This command enables the device to restore a release file and/or a configuration file from a USB storage device.

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

Figure 3-1: Example autoboot.txt file

```
[AlliedWare Plus]
Copy_from_external_media_enabled=yes
Boot_Release=IE340-5.5.1-0.1.rel
Boot_Config=network1.cfg
```

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

Syntax

```
autoboot enable
no autoboot enable
```

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

Mode Global Configuration

Example To enable the Autoboot feature, use the command:

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

Related commands

create autoboot

show autoboot

show boot

boot config-file

Overview Use this command to set the configuration file to use during the next boot cycle.

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

Syntax

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

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

Mode Global Configuration

Usage notes You can only specify that the configuration file is on a USB storage device if there is a backup configuration file already specified in flash. If you attempt to set the configuration file on a USB storage device and a backup configuration file is not specified in flash, the following error message is displayed:

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

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

Examples To run the configuration file “branch.cfg” 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
```

To run the configuration file “branch.cfg” the next time the device boots up, when “branch.cfg” is stored on a USB storage device, use the commands:

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

To stop running the configuration file “branch.cfg” when the device boots up, when “branch.cfg” is stored on a USB storage device, use the commands:

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

Related commands

boot config-file backup

boot system

boot system backup

show boot

boot config-file backup

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

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

Syntax

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

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

Mode Global Configuration

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

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

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

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

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

Related commands

boot config-file

boot system

boot system backup

show boot

boot system

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

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

Syntax

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

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

Mode Global Configuration

Usage notes You can only specify that the release file is on a USB storage device if there is a backup release file already specified in flash. If you attempt to set the release file on a USB storage device and a backup release file is not specified in flash, the following error message is displayed:

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

Examples To boot up with the release file IE340-5.5.1-0.1.rel the next time the device boots up, when the release file is stored on the device's flash filesystem, use the commands:

```
awplus# configure terminal
awplus(config)# boot system flash:/IE340-5.5.1-0.1.rel
```

To run the release file IE340-5.5.1-0.1.rel the next time the device boots up, when the release file is stored on a USB storage device, use the commands:

```
awplus# configure terminal
awplus(config)# boot system usb:/IE340-5.5.1-0.1.rel
```

Related commands

boot config-file

boot config-file backup

boot system backup

show boot

boot system backup

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

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

Syntax

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

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

Mode Global Configuration

Examples To specify the file IE340-5.5.0-2.3.rel as the backup to the main release file, use the commands:

```
awplus# configure terminal
awplus(config)# boot system backup flash:/IE340-5.5.0-2.3.rel
```

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

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

Related commands

boot config-file

boot config-file backup

boot system

show boot

cd

Overview This command changes the current working directory.

Syntax

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

Parameter	Description
<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
- copy files stored on Flash memory to or from a different memory type, such as a USB storage device
- create two copies of the same file on your device

Syntax

```
copy [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 131 for valid syntax.
<destination-name>	The filename and path for the destination file. See Introduction on page 131 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 “newconfig.cfg” onto your device’s Flash from a USB storage device, use the command:

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

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

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

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

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

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

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

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

edit (filename)

show file systems

copy debug

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

Syntax

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

Parameter	Description
<destination-name>	The filename and path where you would like the debug output saved. See Introduction on page 131 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
```

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

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

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

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

Related commands delete debug

move debug

copy running-config

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

Syntax

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

Parameter	Description
<source-name>	The filename and path of a configuration file. This must be a valid configuration file with a **.cfg** filename extension. Specify this when you want the script in the file to become the new running-config. See Introduction on page 131 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 131 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. Specify whether the destination is Flash or USB when loading from the local filesystem.

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 131 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 131 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 131 for valid syntax.

Mode Privileged Exec

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

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

Related commands copy (filename)

show file systems

create autoboot

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

Syntax

```
create autoboot usb
```

Mode Privileged Exec

Example To create an autoboot.txt file on a USB storage device, use the command:

```
awplus# create autoboot usb
```

Related commands

autoboot enable

show autoboot

show boot

crypto verify

Overview Use this command to compare the SHA256 checksum of the release file or bootloader with the correct checksum for the file. This ensures that the release file or bootloader has not been corrupted or interfered with during download.

Use the **no** variant of this command to remove a verified filename/hash combination from the running configuration.

Syntax

```
crypto verify <filename> <hash-value>
crypto verify signed <filename> <hash-value>
crypto verify bootrom <hash-value>
no crypto verify <filename>
```

Parameter	Description
<filename>	The AlliedWare Plus release file that you want to verify
<hash-value>	The known correct checksum of the file. The correct checksum is listed in the release sha256sum file, which is available from the Allied Telesis Download Center.
`signed`	The hash used is from a <release>.sig file and calculated as a keyed HMAC-SHA. Only use this parameter in accordance with the Allied Telesis FIPS Security Policy.
`bootrom`	This tells the device that the signature provided is for the bootrom. It stores that hash permanently, preventing boot if the bootloader is modified.

Default No default

Mode Global Configuration

Usage notes If the verification fails, the following error message will be generated:

```
% Verification Failed
```

If the verification fails, please delete the release file and contact Allied Telesis support.

All models of a particular series run the same release file and therefore have the same checksum. For example, all x930 Series switches have the same checksum.

Once the device has successfully verified the release file, it adds the **crypto verify** command to the running configuration.

If the device is in secure mode, it will verify the release file every time it boots up. To do this, it runs the **crypto verify** command while booting. Therefore, you need to copy the **crypto verify** command to the startup configuration, by using the command **copy running-config startup-config**. If the **crypto verify** command is not in the startup configuration, the device will report a verification error at bootup.

If there is a verification error at bootup, the device produces an error message and finishes booting up. If this happens, run the **crypto verify** command after bootup finishes, to verify the running release file. If verification of the running release file fails, delete the release file and contact Allied Telesis support.

Caution:

When using signature verification, if:

- the release verified is the boot release
- and the device is running in secure mode
- and signed verification succeeds

then the signed hash is also stored into the device and enforced on all subsequent boots.

This means that if you change the software version, the switch will not boot up. You can only change the software version if you reset the switch to the factory defaults **before** changing the software version, by using the command erase factory-default.

Example To verify the release file for 5.4.8-1.2 on an x930 Series switch, use the commands:

```
awplus# configure terminal
awplus(config)# crypto verify x930-5.4.8-1.2.rel
50fae963b460ba02eb0bd609289c0491de404ba5b0d7e5fa79e64f56082ecf
ee
```

Related commands crypto secure-mode

show secure-mode

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 131 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 131 for valid URL syntax.

Mode Privileged Exec

Example To delete debug output, use the following command:

```
awplus# delete debug
```

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

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

Related commands

copy debug

move debug

dir

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

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

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

Mode Privileged Exec

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

```
awplus# dir
```

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

```
awplus# dir flash
```

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

```
awplus# dir all flash:
```

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

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

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

```
awplus# dir sort name
```

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

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

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

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

Output Figure 3-4: Example output from the **dir** command

```
awplus#dir
       630 -rw- May 19 2016 23:36:31  example.cfg
  23652123 -rw- May 17 2016 03:41:18
       149 -rw- Feb  9 2016 00:40:35  exception.log
```

Related commands

cd

pwd

edit

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

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

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

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

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

Syntax

```
edit [<filename>]
```

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

Mode Privileged Exec

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

```
awplus# edit
```

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

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

Related commands edit (filename)

show file

edit (filename)

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

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

Syntax

```
edit <filename>
```

Parameter	Description
<filename>	The filename and path of the remote file. See Introduction on page 131 for valid syntax.

Mode Privileged Exec

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

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

Related commands

copy (filename)

edit

show file

erase 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 131 for valid syntax.
<destination-name>	The filename and path of the destination file. See Introduction on page 131 for valid syntax.

Mode Privileged Exec

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

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

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

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

Related commands

delete

edit

show file

show file systems

move debug

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

Syntax

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

Parameter	Description
<destination-name>	The filename and path where you would like the debug output moved to. See Introduction on page 131 for valid syntax.

Mode Privileged Exec

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

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

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

Output Figure 3-5: 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 autoboot

Overview This command displays the Autoboot configuration and status.

Syntax

```
show autoboot
```

Mode Privileged Exec

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

```
awplus# show autoboot
```

Output Figure 3-6: Example output from the **show autoboot** command

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

Restore information on USB
Autoboot enable in autoboot.txt  : yes
Restore release file             : IE340-5.5.1-0.1.rel (file exists)
Restore configuration file       : network_1.cfg (file exists)
```

Figure 3-7: Example output from the **show autoboot** command when an external media source is not present

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

Related commands

autoboot enable

create autoboot

show boot

show boot

Overview This command displays the current boot configuration.

We recommend that the currently running release is set as the current boot image.

Syntax

```
show boot
```

Mode Privileged Exec

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

```
awplus# show boot
```

Output Figure 3-8: Example output from **show boot**

```
awplus#show boot
Boot configuration
-----------------------------------------------------------------
Current software   : IE340-5.5.1-0.1.rel
Current boot image : flash:/IE340-5.5.1-0.1.rel
Backup  boot image : flash:/IE340-5.5.0-2.3.rel
Default boot config: flash:/default.cfg
Current boot config: flash:/my.cfg (file exists)
Backup  boot config: flash:/backup.cfg (file not found)
Autoboot status    : enabled
```

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

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

Related commands

autoboot enable

boot config-file backup

boot system backup

show autoboot

show file

Overview This command displays the contents of a specified file.

Syntax

```
show file <filename>
```

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

Mode Privileged Exec

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

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

Related commands

edit

edit (filename)

show file systems

show file systems

Overview This command lists the 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 3-9: 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
-----------------------------------------------------------------------
 125.9M    111.8M    flash     rw   flash:      static   local      Y
      -         -    system    rw   system:     virtual  local      -
  10.0M      9.8M    debug     rw   debug:      static   local      Y
   7.0G      4.6G    usbstick  rw   usb:        dynamic  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 nvs usbstick 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 nvs usb 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

edit (filename)

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 3-10: 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 interface

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

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

Syntax

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

Parameter	Description
<interface-list>	The interfaces or ports to display information about. An interface-list can be: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • the loopback interface (lo) • a continuous range of interfaces separated by a hyphen (e.g. vlan10-20) • a comma-separated list (e.g. vlan1,vlan10-20). 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 ports 1 to 4, use the command:

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

To display the current running configuration of a device for vlan2, use the command:

```
awplus# show running-config interface vlan2
```

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

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

Output Figure 3-11: Example output from **show running-config interface** for a switchport

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

Related commands

copy running-config

show running-config

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 3-12: Example output from the **show startup-config** command

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

...

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

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

show version

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

Syntax

```
show version
```

Mode User Exec and Privileged Exec

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

```
awplus# show version
```

Related commands boot system backup

show boot

unmount

Overview Use this command to unmount an external storage device. We recommend you unmount storage devices before removing them, to avoid file corruption. This is especially important if files may be automatically written to the storage device, such as external log files or AMF backup files.

Syntax

```
unmount usb
```

Parameter	Description
`usb`	Unmount the USB storage device.

Mode Privileged Exec

Example To unmount a USB storage device and safely remove it from the device, use the command:

```
awplus# unmount usb
```

Related commands

clear log external

log external

show file systems

show log config

show log external

Command changes Version 5.4.7-1.1: 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 185
- "aaa local authentication attempts lockout-time" on page 186
- "aaa local authentication attempts max-fail" on page 187
- "aaa login fail-delay" on page 188
- "clear aaa local user lockout" on page 189
- "clear line console" on page 190
- "clear line vty" on page 191
- "enable password" on page 192
- "enable secret (deprecated)" on page 195
- "exec-timeout" on page 196
- "flowcontrol hardware (asyn/console)" on page 198
- "length (asyn)" on page 200
- "line" on page 201
- "privilege level" on page 203
- "security-password history" on page 204
- "security-password forced-change" on page 205
- "security-password lifetime" on page 206
- "security-password min-lifetime-enforce" on page 207
- "security-password minimum-categories" on page 208
- "security-password minimum-length" on page 209

- "security-password reject-expired-pwd" on page 210
- "security-password warning" on page 211
- "service advanced-vty" on page 212
- "service password-encryption" on page 213
- "service telnet" on page 214
- "show aaa local user locked" on page 215
- "show privilege" on page 216
- "show security-password configuration" on page 217
- "show security-password user" on page 218
- "show telnet" on page 219
- "show users" on page 220
- "telnet" on page 221
- "telnet server" on page 222
- "terminal length" on page 223
- "terminal resize" on page 224
- "username" on page 225

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

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

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 console

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

Syntax

```
clear line console 0
```

Mode Privileged Exec

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

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

Related commands

clear line vty

flowcontrol hardware (asyn/console)

line

show users

clear line vty

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

Syntax

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

Parameter	Description
<0-32>	Line number

Mode Privileged Exec

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

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

Related commands

privilege level

line

show telnet

show users

enable password

Overview 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.

Secure mode In secure mode, the **enable password** command allows changing privilege level up to the level configured for the current user, and will require a password if one has been configured for that privilege level.

Syntax

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

Parameter	Description
<password>	Specifies the unencrypted password.
8	Specifies that an encrypted password will follow.
<encrypted-password>	Specifies the encrypted password.
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. There are three methods to enable a password. In the examples below, for each method, note that the configuration is different and the configuration file output is different, but the password string to be used to enter the Privileged Exec mode with the **enable** command is the same (in this example, **mypasswd**).

A user can have an intermediate CLI security level set with this command for privilege level 7 to access all the show commands in Privileged Exec mode and all

the commands in User Exec mode, but not any configuration commands in Privileged Exec mode.

Entering plaintext passwords

The plaintext password is a clear text string that appears in the configuration file as configured. For example:

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

This results in the following show output, with the password shown in plaintext:

```
awplus#show run
Current configuration:
...
hostname awplus
enable password mypasswd
...
```

Entering encrypted passwords

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

For example:

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

This results in the following show output:

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

Entering pre-encrypted passwords

You can configure an encrypted password using the **<encrypted-password>** parameter (**8**). Use this method if you already know the encrypted string corresponding to the plaintext string that you want to use as a password. You do not have to use the service password-encryption command with this method. The

output in the configuration file will show only the encrypted string, and not the text string. For example:

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

This results in the following show output:

```
awplus#show run
Current configuration:
...
hostname awplus
enable password 8 fU7zHzuutY2SA
...
```

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
```

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

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

Validation Commands show running-config

Related commands

line

service telnet

flowcontrol hardware (asyn/console)

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

Syntax

```
flowcontrol hardware
no flowcontrol hardware
```

Mode Line Configuration

Default Hardware flow control is disabled by default.

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

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

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

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

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

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

Examples

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

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

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

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

Related commands

clear line console

show running-config

speed (asyn)

length (asyn)

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

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

Syntax

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

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

Mode Line Configuration

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

Usage 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 the console to 10 rows, use the command:

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

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

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

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

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

Related commands terminal resize

terminal length

line

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

Syntax

```
line vty <first-line> [<last-line>]
line console 0
```

Parameter	Description
<first-line>	*<0-32>* Specify the first line number.
<last-line>	*<0-32>* Specify the last line number.
`console`	The console terminal line(s) for local access.
`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 speed (asyn), length (asyn), privilege level, and authentication (login authentication) or accounting (accounting login) method lists.

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

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

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

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

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

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

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

Related commands

accounting login

clear line console

clear line vty

flowcontrol hardware (asyn/console)

length (asyn)

login authentication

privilege level

speed (asyn)

privilege level

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

Syntax

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

Mode Line Configuration

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

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

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

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

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

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

Related commands

enable password

line

show privilege

username

security-password history

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

The **no** 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.

NOTE: *Do not use encrypted passwords for GUI users. The GUI requires unencrypted user passwords only - not encrypted user passwords. Do not use option 8 for GUI users.*

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 current number of failed attempts, last failure time and location against each user account attempting to log into the device.

Note that once the lockout count has been manually cleared by another privileged account using the clear aaa local user lockout command or a locked account successfully logs into the system after waiting for the lockout time, this command will display nothing for that particular account.

Syntax

```
show aaa local user locked
```

Mode User Exec and Privileged Exec

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

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

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

```
awplus# show aaa local user locked
Login           Failures Latest failure     From
bob                  3    05/23/14 16:21:37  ttyS0
manager              5    05/23/14 16:31:44  192.168.1.200
```

Related commands

aaa local authentication attempts lockout-time

aaa local authentication attempts max-fail

clear aaa local user lockout

show 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.

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	Specifies that you are entering a password as a string that has already been encrypted, instead of entering a plain-text password. The running-config displays the new password as an encrypted string even if password encryption is turned off. Note that the user enters the plain-text version of the password when logging in.
	<password>	The user's password. The password can be up to 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 Feature Licensing Commands

Introduction

Overview

This chapter provides an alphabetical reference for each of the Feature Licensing commands. Feature Licensing enables you to use advanced features such as Layer 3 routing.

NOTE: *Feature licensing is not available in Secure Mode (see the crypto secure-mode command.*

To see which Feature Licenses are available for your device, see the AlliedWare Plus Datasheet.

Allied Telesis Management Framework (AMF) requires a Subscription License. For information about Subscription Licensing commands, see the Subscription Licensing Commands chapter.

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

Command List

- "license" on page 228
- "show license" on page 230
- "show license brief" on page 232

license

Overview This command activates the licensed software feature set on a device.

Use the **no** variant of this command to deactivate the licensed software feature set on a device.

For feature licenses, contact your authorized distributor or reseller. If a license key expires or is incorrect so the license key is invalid, then some software features will be unavailable.

NOTE: *See the AlliedWare Plus™ datasheet for a list of current feature licenses available by product. Purchase licenses from your authorized dealer or reseller.*

NOTE: *The **license** command is not available in Secure Mode (see the crypto secure-mode command.*

In a live network, only install feature licenses during scheduled maintenance. For example, if a feature license includes EPSR, installing that license will cause EPSR to be restarted with a temporary loss of EPSR network traffic.

Syntax

```
license <label> <key>
no license <label>
```

Parameter	Description
<label>	A name for the feature license. To determine names already in use, use the show license command. This can be the default name supplied for the feature, or a renamed feature name.
<key>	The encrypted license key to enable a set of software features.

Mode Privileged Exec

Usage notes You can change the license label using this command to make it specific to you when you initially add a license. Once a license is added, any change to the license label first requires removal of the license before adding a license again with a new license label.

The default feature license labels are issued along with encrypted license keys by e-mail for you to apply using this command to activate features. You can change default feature license labels, but they must be 15 characters or less.

For example, you may want to change the label of the premium license to “premium-license”. You can check your new license label by using the show license command.

If you add a feature license you will be prompted at the console that the feature needs to restart. Restarting of individual protocols in this manner could result in the loss of network traffic. Only install licenses in scheduled maintenance periods for devices in a live environment.

For example, if the feature license contains a license for the EPSR protocol, then that protocol will restart, but you do not need to manually restart the whole device for the new license to take effect.

Examples

To activate the license called “Premium” that has the key 12345678ABCDE123456789ABCDE, use the command:

```
awplus# license Premium 12345678ABCDE123456789ABCDE
```

To deactivate the license called “Premium”, use the command:

```
awplus# no license Premium
```

Related commands

show license

show license

Overview This command displays information about a specific software feature license, or all enabled software feature licenses on the device.

Syntax

```
show license [feature] [<label>|index <index-number>]
```

Parameter	Description
`feature`	Only display license information for any applied feature licenses.
`<label>`	The license name to show information about. This can be used instead of the index number to identify a specific license.
`index <index-number>`	The index number of the license to show information about. This can be used instead of the license name to identify a specific license.

Mode User Exec and Privileged Exec

Examples To display full information about all enabled licenses, use the command:

```
awplus# show license
```

To display full information about the licenses with index number 1, use the command:

```
awplus# show license index 1
```

Output Figure 5-1: Example output from **show license**

```
awplus#show license
Board region: Global
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : Base License
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 20-Mar-2019
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100, ...
```

Table 5-1: Parameters in the output of **show license**

Parameter	Description
Board region	Name of the region for the Base License features.
Index	Index identifying entry. The index is assigned automatically by the software. It is not configured.

Table 5-1: Parameters in the output of **show license** (cont.)

Parameter	Description
License name	Name of the license key bundle (case-sensitive).
Customer name	Customer name.
Quantity of licenses	Quantity of licensed installations.
Type of license	Full or Trial.
License issue date	Date the license was generated.
License expiry date	Expiry date for trial license.
Features included	List of features included in the feature license.

Related commands

license

show license brief

show license brief

Overview This command displays information about a specific software feature license, or all enabled software feature licenses on the device.

Syntax

```
show license brief
show license [feature] [<label>|index <index-number>] brief
```

Parameter	Description
`feature`	Only display license information for any applied feature licenses.
`<label>`	The license name to show information about. This can be used instead of the index number to identify a specific license.
`index <index-number>`	The index number of the license to show information about. This can be used instead of the license name to identify a specific license.
`brief`	Displays a brief summary of license information.

Mode User Exec and Privileged Exec

Examples To display a brief summary of information about all licenses, use the command:

```
awplus# show license brief
```

Output Figure 5-2: Example output from **show license brief**

```
awplus#show license brief
Board region: Global
Software Licenses
-------------------------------------------------------------------------
Index License name    Quantity     Customer name
      Type            Version      Period
-------------------------------------------------------------------------
1     Base License    1            Base License
      Full                         N/A

Current enabled features for displayed licenses:
 IPv6Basic, LAG-FULL, MLDSnoop ...
```

Table 5-2: Parameters in the output of **show license brief**

Parameter	Description
Board region	Name of the region for the Base License features.
Index	Index identifying entry. The index is assigned automatically by the software. It is not configured.

Table 5-2: Parameters in the output of **show license brief** (cont.)

Parameter	Description
License name	Name of the license key bundle (case-sensitive).
Quantity	Quantity of licensed installations.
Customer name	Customer name.
Type	Full or Trial.
Period	Expiry date for trial license.
Current enabled features for displayed licenses	List of features included in the license.

Related commands

license

show license

6 Subscription Licensing Commands

Introduction

Overview

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

Subscription Licensing enables you to use OpenFlow. To see the OpenFlow 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 235
- "license update online" on page 236
- "show license external" on page 237

license update file

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

Only use this command if you cannot directly access the Allied Telesis Download Center from this device. Otherwise, use the command license update online instead.

Syntax

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

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

Mode Privileged Exec

Usage notes You can download subscription licenses from the Allied Telesis Download Center, in order to copy them onto the device.

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

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

Related commands license update online

show license external

Command changes Version 5.4.6-2.1: usage changed by introduction of license update online

license update online

Overview Use this command to add or update subscription licenses from the Allied Telesis Download Center, to subscribe to features such as AMF master and OpenFlow.

When you enter this command, the device will:

1) Connect to the Download Center

2) Check if new or changed licenses are available for the device, keyed to the device's serial number

3) For each such license it finds, download and install the license.

Syntax

```
license update online
```

Default AlliedWare Plus devices do not automatically connect to the Download Center and check whether licenses are available. They only check when you run the **license update online** command.

Mode User Exec/Privileged Exec

Usage notes

Verifying the update

The update process normally takes approximately 5 seconds.

If the console does not respond for 10 or more seconds after typing the command, a network, routing or firewall configuration error is probably preventing the connection from establishing. If this happens, you can abort the command by pressing Ctrl-C, or wait for the command to time out after 30 seconds.

If the connection to the Download Centers fails and times out, an error message will be generated on the CLI to indicate the problem. If you abort the command, no error message is displayed.

If the update is successful, the device will produce log messages to say which features have had their licensing state updated (activated, deactivated, number of items changed, or expiry date changed). If the command completes successfully but there are no licenses available for the device, or no change in the licenses already on the device, no log messages will be produced.

You should also use the show license external command to confirm which licenses are active on the device after the update has been applied.

Example To add a subscription license, use the command:

```
awplus# license update online
```

Related commands show license external

Command changes Version 5.4.6-2.1: command added

show license external

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

Syntax

```
show license external
```

Mode Privileged Exec

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 online

7 System Configuration and Monitoring Commands

Introduction

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

Command List

- "banner exec" on page 240
- "banner login (system)" on page 242
- "banner motd" on page 244
- "clock set" on page 246
- "clock summer-time date" on page 247
- "clock summer-time recurring" on page 249
- "clock timezone" on page 251
- "continuous-reboot-prevention" on page 252
- "crypto secure-mode" on page 254
- "debug core-file" on page 255
- "ecofriendly led" on page 256
- "ecofriendly lpi" on page 257
- "findme" on page 259
- "findme trigger" on page 261
- "hostname" on page 262
- "max-fib-routes" on page 264
- "max-static-routes" on page 265
- "no debug all" on page 266
- "reboot" on page 268
- "reload" on page 269

- "show clock" on page 270
- "show continuous-reboot-prevention" on page 272
- "show cpu" on page 273
- "show cpu history" on page 276
- "show debugging" on page 278
- "show ecofriendly" on page 279
- "show interface memory" on page 281
- "show memory" on page 283
- "show memory allocations" on page 285
- "show memory history" on page 287
- "show memory pools" on page 288
- "show memory shared" on page 289
- "show process" on page 290
- "show reboot history" on page 292
- "show router-id" on page 293
- "show secure-mode" on page 294
- "show system" on page 295
- "show system environment" on page 296
- "show system environment counters" on page 297
- "show system interrupts" on page 299
- "show system mac" on page 300
- "show system pci device" on page 301
- "show system pci tree" on page 302
- "show system serialnumber" on page 303
- "show tech-support" on page 304
- "speed (asyn)" on page 306
- "terminal monitor" on page 308
- "undebug all" on page 309

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) 5.5.1 04/05/21 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) 5.5.1 04/05/21 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 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) 5.5.1 04/05/21 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) 5.5.1 04/05/21 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) 5.5.1 04/05/21 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) 5.5.1 04/05/21 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

continuous-reboot-prevention

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

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

Syntax

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

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

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

Mode Global Configuration

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

Examples

To enable continuous reboot prevention, use the commands:

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

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

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

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

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

To disable continuous reboot prevention, use the commands:

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

Related commands

show continuous-reboot-prevention

show reboot history

show tech-support

crypto secure-mode

Overview Use this command to put the device into Secure Mode. When in Secure Mode, the following are disabled:

- Telnet
- SSHv1
- SNMPv1/v2
- All privilege levels except 1 and 15
- Algorithms that are not supported under FIPS, including MD5, RSA-1 and DSA
- The ability to store passwords in cleartext and to specify an **enable** password.

In Secure Mode, the web server on the device (used by the Device GUI) only accepts AES128-SHA ciphers.

Note: Stacking is not supported in Secure Mode.

Use the **no** variant of this command to leave Secure Mode. You should delete all sensitive information first; see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
crypto secure-mode
no crypto secure-mode
```

Default By default, the device is not in Secure Mode.

Mode Global Configuration

Example For step-by-step instructions about how to enter and leave Secure Mode, see "How to Enable Secure Mode" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Related commands

boot system

crypto key zeroize

crypto pki trustpoint

crypto verify

show secure-mode

Command changes

Version 5.4.6-1.1: command added to x930 Series

Version 5.4.8-1.2: command added to x220, XS900MX, x550 Series

Version 5.4.8-2.1: command added to SBx908 GEN2, x950 Series

debug core-file

Overview Use this command to enable the generation of crash core files.

Use the **no** variant of this command to disable the generation of crash core files.

Syntax

```
debug core-file
no debug core-file
```

Default Enabled.

Mode Global Configuration

Usage notes Core files may contain raw memory content. This may not be acceptable in a security certified network. Use the **no debug core-file** command to prevent such core files from being generated.

Example To prevent the generation of core files, use the commands:

```
awplus# configure terminal
awplus(config)# no debug core-file
```

Related commands show system

Command changes Version 5.4.9-1.0: command added

ecofriendly led

Overview Use this command to enable the eco-friendly LED (Light Emitting Diode) feature, which turns off power to the port LEDs.

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

Syntax

```
ecofriendly led
no ecofriendly led
```

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

Mode Global Configuration

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

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

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

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

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

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

Related commands ecofriendly lpi

show ecofriendly

ecofriendly lpi

Use this command to conserve power by enabling the eco-friendly LPI (Low Power Idle) feature. This feature reduces the power supplied to the ports by the switch whenever the ports are idle and are connected to IEEE 802.3az Energy Efficient Ethernet compliant host devices.

LPI is a feature of the IEEE 802.3az Energy Efficient Ethernet (EEE) standard. LPI lowers power consumption of switch ports during periods of low link utilization when connected to IEEE 802.3az compliant host devices. If no data is sent then the switch port can enter a sleep state, called Low Power Idle (LPI), to conserve power used by the switch.

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

Syntax

```
ecofriendly lpi
no ecofriendly lpi
```

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

Mode Interface Configuration for a switch port, or Interface Configuration for a range of switch ports.

Usage notes For an example of how to configure a trigger to enable the eco-friendly LPI feature, see the Triggers Feature Overview and Configuration Guide.

All ports configured for LPI must support LPI in hardware and must be configured to auto negotiate by default or by using the speed and duplex commands as needed.

Examples To enable the eco-friendly LPI feature on a switch port, port1.0.2, use the following commands:

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

To enable the eco-friendly LPI feature on a range of switch ports, port1.0.2-port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# ecofriendly lpi
```

To disable the eco-friendly feature on port1.0.2, use the following commands:

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

Related commands

duplex

ecofriendly led

show ecofriendly

show interface

speed

findme

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

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

Syntax

```
findme [interface <port-list>] [timeout <duration>]
no findme
```

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

Default By default all port LEDs flash for 60 seconds.

Mode Privileged Exec

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

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

```
awplus# findme
```

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

```
awplus# findme timeout 120
```

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

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

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

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

```
awplus# no findme
```

findme trigger

Overview When this command is enabled, the LED flashing functionality of the **find-me** command is applied whenever any or all of the selected parameter conditions is detected.

Use the **no** variant to remove the findme trigger function for the selected parameter.

Syntax

```
findme trigger {all|loopprot|thrash-limit|qsp}
no findme trigger {all|loopprot|thrash-limit|qsp}
```

Parameter	Description
`all`	Enable the find-me function whenever any of the listed parameter conditions are detected
`loopprot`	Enable the findme function whenever a loop protection condition is detected.
`thrash-limit`	Enable the findme function whenever a MAC address thrash-limiting condition is detected.
`qsp`	Enable the findme function whenever a QoS Storm Protection condition is detected.

Default The findme trigger function is disabled.

Mode Global config

Usage notes Note that findme trigger is not available if you have set the switch to take the following actions in response to an event:

- For loop detection, the actions **log-only** and **none**
- For MAC address thrash-limiting, the actions **learn-disable** and **none**.

Example To enable action LED flashing for the loop protection function:

```
awplus# findme trigger loopprot
```

Related commands

findme

loop-protection loop-detect

storm-protection

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. This is also referred to as the Node name in AMF output screens.

Default `awplus`

Mode Global Configuration

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

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

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

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

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

This changes the prompt to:

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

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

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

This changes the prompt to:

```
awplus(config)#
```

NOTE: *When AMF is configured, running the* ***no hostname*** *command will apply a hostname that is based on the MAC address of the device node, for example,* ***node_0000_5e00_5301****.*

Related commands show system

max-fib-routes

Overview This command enables you to control the maximum number of FIB routes configured. It operates by providing parameters that enable you to configure preset maximums and warning message thresholds.

NOTE: *For static routes use the max-static-routes command.*

Use the **no** variant of this command to set the maximum number of FIB routes to the default of 4294967294 FIB routes.

Syntax

```
max-fib-routes <1-4294967294> [<1-100>|warning-only]
no max-fib-routes
```

Parameter	Description
`max-fib-routes`	This is the maximum number of routes that can be stored in the device's Forwarding Information dataBase. In practice, other practical system limits would prevent this maximum being reached.
<1-4294967294>	The allowable configurable range for setting the maximum number of FIB-routes.
<1-100>	This parameter enables you to optionally apply a percentage value. This percentage will be based on the maximum number of FIB routes you have specified. This will cause a warning message to appear when your routes reach your specified percentage value. Routes can continue to be added until your configured maximum value is reached.
`warning-only`	This parameter enables you to optionally apply a warning message. If you set this option a warning message will appear if your maximum configured value is reached. Routes can continue to be added until your device reaches either the maximum capacity value of 4294967294, or a practical system limit.

Default The default number of FIB routes is the maximum number of FIB routes (4294967294).

Mode Global Configuration

Examples To set the maximum number of dynamic routes to 2000 and warning threshold of 75%, use the following commands:

```
awplus# config terminal
awplus(config)# max-fib-routes 2000 75
```

max-static-routes

Overview Use this command to set the maximum number of static routes, excluding FIB (Forwarding Information Base) routes.

NOTE: *For FIB routes use the max-fib-routes command.*

Use the **no** variant of this command to set the maximum number of static routes to the default of 1000 static routes.

Syntax

```
max-static-routes <1-1000>
no max-static-routes
```

Default The default number of static routes is the maximum number of static routes (1000).

Mode Global Configuration

Example To reset the maximum number of static routes to the default maximum, use the command:

```
awplus# configure terminal
awplus(config)# no max-static-routes
```

NOTE: *Static routes are applied before adding routes to the RIB (Routing Information Base). Therefore, rejected static routes will not appear in the running config.*

Related commands max-fib-routes

no debug all

Overview This command disables the debugging facility for all features on your device. This stops the device from generating any diagnostic debugging messages.

You can optionally disable the debugging facility for only the given protocol or feature. The features available depend on your device and will be a subset of the features listed in the Syntax section below.

Syntax

```
no debug all [bgp|ipv6 ospf|ipv6 rip|dot1x|nsm|ospf|pim
dense-mode|pim sparse-mode|rip|vrrp]
```

Parameter	Description
`bgp`	Turns off all debugging for BGP (Border Gateway Protocol).
`dot1x`	Turns off all debugging for IEEE 802.1X port-based network access- control.
`ipv6 ospf`	Turns off all debugging for IPv6 OSPF (Open Shortest Path First).
`ipv6 rip`	Turns off all debugging for IPv6 RIP (Routing Information Protocol).
`nsm`	Turns off all debugging for the NSM (Network Services Module).
`ospf`	Turns off all debugging for OSPF (Open Shortest Path First).
`pim dense-mode`	Turns off all debugging for PIM (Protocol Independent Multicast) Dense Mode.
`pim sparse-mode`	Turns off all debugging for PIM (Protocol Independent Multicast) Sparse Mode.
`rip`	Turns off all debugging for RIP (Routing Information Protocol).
`vrrp`	Turns off all debugging for VRRP (Virtual Router Redundancy Protocol).

Default Disabled

Mode Global Configuration and Privileged Exec

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

```
awplus# no debug all
```

To disable all BGP debugging, use the command:

```
awplus# no debug all bgp
```

To disable all 802.1X debugging, use the command:

```
awplus# no debug all dot1x
```

To disable all NSM debugging, use the command:

```
awplus# no debug all nsm
```

To disable all OSPF debugging, use the command:

```
awplus# no debug all ospf
```

To disable all PIM Dense Mode debugging, use the command:

```
awplus# no debug all pim dense-mode
```

To disable all PIM Sparse Mode debugging, use the command:

```
awplus# no debug all pim sparse-mode
```

To disable all RIP debugging, use the command:

```
awplus# no debug all rip
```

To disable all VRRP debugging, use the command:

```
awplus# no debug all vrrp
```

Related commands undebug all

Command changes Version 5.4.7-1.1: **pim dense-mode**, **pim sparse-mode**, and **rip** parameters added

reboot

Overview This command halts the device and performs a cold restart (also known as reload). It displays a confirmation request before restarting.

Syntax

```
reboot
reload
```

Mode Privileged Exec

Usage notes The **reboot** and **reload** commands perform the same action.

Examples To restart the device, use the command:

```
awplus# reboot
reboot system? (y/n): y
```

reload

Overview This command performs the same function as the reboot command.

show 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 7-1: 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 continuous-reboot-prevention

Overview This command displays the current continuous reboot prevention configuration.

Syntax

```
show continuous-reboot-prevention
```

Mode User Exec and Privileged Exec

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

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

Output Figure 7-2: Example output from the **show continuous-reboot-prevention** command

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

Related commands

continuous-reboot-prevention

show reboot history

show cpu

Overview This command displays a list of running processes with their CPU utilization.

For information on filtering and saving command output, see 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 7-3: 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 7-4: 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 7-5: 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

BGP debugging status:
  BGP debugging is off
  BGP nsm debugging is off
  BGP events debugging is off
  BGP keepalives debugging is off
  BGP updates debugging is off
  BGP fsm debugging is off
  BGP filter debugging is off
  BGP Route Flap Dampening debugging is off

802.1X debugging status:

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

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

show ecofriendly

Overview This command displays the switch's eco-friendly configuration status. The ecofriendly led and ecofriendly lpi configuration status are shown in the show ecofriendly output.

Syntax

```
show ecofriendly
```

Mode Privileged Exec and Global Configuration

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

```
awplus# show ecofriendly
```

Output Figure 7-6: Example output from the **show ecofriendly** command

```
awplus#show ecofriendly
Front panel port LEDs          normal
Energy efficient ethernet
Port          Name             Configured  Status
port1.0.1     Port 1           lpi         lpi
port1.0.2                      lpi         lpi
port1.0.3                      lpi         lpi
port1.0.4                      off         off
port1.0.5                      lpi         off
port1.0.6     Port 6           off         off
port1.0.7                      off         -
port1.0.8                      off         -
port1.0.9                      off         -
port1.0.10                     off         -
...
```

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

Parameter	Description
`normal`	The eco-friendly LED feature is disabled and port LEDs show the current state of the ports. This is the default setting.
`off`	The eco-friendly LED feature is enabled and power to the port LEDs is disabled.
`normal (configuration overridden by eco button)`	The eco-friendly LED feature has been disabled with the eco-switch button, overriding the configuration set with the ecofriendly led command. The port LEDs show the current state of the ports.

Table 3: Parameters in the output of the **show ecofriendly** command (cont.)

Parameter	Description
`off (configuration overridden by eco button)`	The eco-friendly LED feature has been enabled with the eco-switch button, overriding the configuration set with the ecofriendly led command. Power to the port LEDs is disabled.
`Port`	Displays the port number as assigned by the switch.
`Name`	Displays the port name if a name is configured for a port number.
`Configured`	The eco-friendly LPI feature is configured on the port. Either LPI or off is displayed.
`Status`	The eco-friendly LPI feature is active on the port. Either LPI or off is displayed. Ports that are not running show a dash (-).

Related commands

ecofriendly led

ecofriendly lpi

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: • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • 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.

Mode User Exec and Privileged Exec

Example To display the shared memory used by all interfaces, use the command:

```
awplus# show interface memory
```

To display the shared memory used by port1.0.1 and port1.0.3 to port1.0.4, use the command:

```
awplus# show interface port1.0.1,port1.0.3-port1.0.4 memory
```

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

```
awplus#show interface memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
port1.0.1    491535       512            1
port1.0.2    393228       512            1
port1.0.3    557073       512            1
...
lo           425997       512            1
po1          1179684      512            1
po2          1212453      512            1
sa3          1245222      512            1
```

Figure 7-8: Example output from **show interface <port-list> memory** for a list of interfaces

```
awplus#show interface port1.0.1,port1.0.3-port1.0.4 memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
port1.0.1    589842       512            1
port1.0.3    688149       512            1
port1.0.4    327690       512            1
```

Related commands

show interface brief

show interface status

show interface switchport

show memory

Overview This command displays the memory used by each process that is currently running.

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

Syntax

```
show memory [sort {size|peak|stk}]
```

Parameter	Description	
`sort`	Changes the sorting order for the list of processes. If you do not specify this, then the list is sorted by percentage memory utilization.	
	`size`	Sort by the amount of memory the process is currently using.
	`peak`	Sort by the amount of memory the process is currently using.
	`stk`	Sort by the stack size of the process.

Mode User Exec and Privileged Exec

Example To display the memory used by the current running processes, use the command:

```
awplus# show memory
```

Output Figure 7-9: Example output from **show memory**

```
awplus#show memory sort stk

RAM total: 124384 kB; free: 64236 kB; buffers: 15888 kB

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

Table 4: Parameters in the output of the **show memory** command

Parameter	Description
`RAM total`	Total amount of RAM memory free.
`free`	Available memory size.
`buffers`	Memory allocated kernel buffers.
`pid`	Identifier number for the process.
`name`	Short name used to describe the process.
`mem%`	Percentage of memory utilization the process is currently using.
`size`	Amount of memory currently used by the process.
`peak`	Greatest amount of memory ever used by the process.
`data`	Amount of memory used for data.
`stk`	The stack size.

Related commands

show memory allocations

show memory history

show memory pools

show memory shared

show memory allocations

Overview This command displays the memory allocations used by processes.

For information on filtering and saving command output, see 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 7-10: Example output from the **show memory allocations** command

```
awplus#show memory allocations
Memory allocations for imi
----------------------------

Current 15093760 (peak 15093760)

Statically allocated memory:
 - binary/exe                :    1675264
 - libraries                 :    8916992
 - bss/global data           :    2985984
 - stack                     :     139264

Dynamically allocated memory (heap):
 - total allocated           :    1351680
   - in use                  :    1282440
   - non-mmapped             :    1351680
 - maximum total allocated   :    1351680
 - total free space          :      69240
   - releasable              :      68968
   - space in freed fastbins :         16

Context
           filename:line   allocated      freed
 +            lib.c:749          484
.
.
.
```

Related commands

show memory

show memory history

show memory pools

show memory shared

show tech-support

show memory history

Overview This command prints a graph showing the historical memory usage.

For information on filtering and saving command output, see 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 7-11: Example output from the **show memory history** command

```
Per minute memory utilization history

100
 90
 80
 70
 60
 50
 40************************************************************
 30
 20
 10
    |....|....|....|....|....|....|....|....|....|....|....|....
    Oldest                                                  Newest
        Memory utilization% per minute (last 60 minutes)
              * = average memory utilisation%.
...
```

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 7-12: Example output from the **show memory pools** command

```
awplus#show memory pools
Memory pools for imi
----------------------

Current 15290368 (peak 15290368)

Statically allocated memory:
 - binary/exe                 :    1675264
 - libraries                  :    8916992
 - bss/global data            :    2985984
 - stack                      :     139264

Dynamically allocated memory (heap):
 - total allocated            :    1548288
   - in use                   :    1479816
   - non-mmapped              :    1548288
 - maximum total allocated    :    1548288
 - total free space           :      68472
   - releasable               :      68200
   - space in freed fastbins  :         16
.
.
.
```

Related commands

show memory allocations

show memory history

show tech-support

show memory shared

Overview This command displays shared memory allocation information. The output is useful for diagnostic purposes by Allied Telesis authorized service personnel.

For information on filtering and saving command output, see 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 7-13: Example output from the **show memory shared** command

```
awplus#show memory shared
Shared Memory Status
--------------------------
Segment allocated  = 39
Pages allocated    = 39
Pages resident     = 11

Shared Memory Limits
--------------------------
Maximum number of segments          = 4096
Maximum segment size (kbytes)       = 32768
Maximum total shared memory (pages) = 2097152
Minimum segment size (bytes)        = 1
```

Related commands

show memory allocations

show memory history

show memory

show process

Overview This command lists a summary of the current running processes.

For information on filtering and saving command output, see 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 7-14: 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 5: 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 7-15: 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 6: Parameters in the output from the **show reboot history** command

Parameter	Description
`Unexpected`	A non-intended reboot. The reboot is counted by the continuous reboot prevention feature, as long as the reboot occurred in the time period specified for continuous reboot prevention.
`Expected`	A planned or user-triggered reboot. The reboot is not counted by the continuous reboot prevention feature.
`Continuous reboot prevention`	A continuous reboot prevention event has occurred. The action taken is configured with the **continuous-reboot-prevention** command. The next time period during which reboot events are counted begins from this event.
`User request`	User initiated reboot via the CLI.

Related commands

show continuous-reboot-prevention

show tech-support

show router-id

Overview Use this command to show the Router ID of the current system.

Syntax

```
show router-id
```

Mode User Exec and Privileged Exec

Example To display the Router ID of the current system, use the command:

```
awplus# show router-id
```

Output Figure 7-16: Example output from the **show router-id** command

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

show secure-mode

Overview Use this command to see whether secure mode is enabled or not. Secure mode disables a number of insecure features, such as Telnet.

Syntax

```
show secure-mode
```

Mode User Exec/Privileged Exec

Example To see if secure mode is enabled, use the command:

```
awplus# show secure-mode
```

Output Figure 7-17: Example output from **show secure-mode**

```
awplus#show secure-mode
Secure mode is enabled
```

Related commands crypto secure-mode

show system

Overview This command displays 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 AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax
```
show system
```

Mode User Exec and Privileged Exec

Example To display configuration information, use the command:

```
awplus# show system
```

Output Figure 7-18: Example output from **show system**

```
System Status                                          Mon Sep 28 08:42:16 2020

Board      ID   Bay     Board Name                        Rev   Serial number
-------------------------------------------------------------------------------
Base       542  Base    IE340-20GP                        A-0   A10248H190400025
-------------------------------------------------------------------------------
RAM: Total: 466520 kB Free: 330832 kB
Flash: 125.9MB Used: 14.1MB Available: 111.8MB
-------------------------------------------------------------------------------
Environment Status : Normal
Uptime             : 0 days 00:08:09
Bootloader version : 6.2.18

Current software   : IE340-5.5.0-1.3.rel
Software version   : 5.5.0-1.3
Build date         : Wed Sep 9 21:10 UTC 2020

Current boot config: flash:/default.cfg (file exists)

System Name
 awplus
System Contact
```

Related commands show system environment

show system environment

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

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

Syntax

```
show system environment
```

Mode User Exec and Privileged Exec

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

```
awplus# show system environment
```

Output Figure 7-19: Example output from **show system environment**

```
awplus#show sys environment
Environment Monitoring Status

Overall Status: Normal

Resource ID: 1  Name: IE340-20GP
ID  Sensor (Units)                    Reading  Low Limit High Limit Status
1   Temp: System (Degrees C)               29   85(Hyst)         90     Ok
2   Voltage: Input 1 (Volts)           53.686     52.500     57.000     Ok
3   Voltage: Input 2 (Volts)           53.686     52.500     57.000     Ok
4   Almmon: LED Output                     No          -          -      Ok
5   Contact Input 1                      Open          -          -      Ok
6   Almmon: Relay Output 1             Closed          -          -      Ok
7   Power Input 1                          No          -          -      Ok
8   Power Input 2                          No          -          -      Ok
```

Related commands

show system

show system environment counters

show system environment counters

Overview Use this command to see the environmental sensor counters.

Syntax

```
show system environment counters
```

Mode User Exec and Privileged Exec

Example To show the environment sensor counters, use the following command:

```
awplus# show system environment counters
```

Output Figure 7-20: Example output from **show system environment counters**

```
awplus#show system environment counters
Environment Monitoring Counters

Resource ID: 1  Name: IE340-12GP
ID Sensor                    Value    Threshold Checked  Read   Alarm    Alarm
                             readings readings  readings errors asserted cleared
1  Temp: System                   16         23        0      0        0       0
2  Voltage: Input 1               17         32        0      0        1       0
3  Voltage: Input 2               17         32        0      0        1       0
4  Almmon: LED Output             24          0        0      0        0       0
5  Contact Input 1                16          0        0      0        0       0
6  Almmon: Relay Output 1         17          0        0      0        0       0
7  Power Input 1                  16          0        0      0        0       0
8  Power Input 2                  16          0        0      0        0       0
```

Table 7-1: Parameters in the output from **show system environment counters**

Parameter	Description
Value readings	Number of times that the value of this sensor has been read.
Threshold readings	Number of times that a threshold value related to this sensor has been read.
Checked readings	Number of times that this sensor has gone outside a threshold and has been re-read to confirm this is a genuine error.
Read errors	Number of times that there was an error returned when reading this sensor or one of its threshold values.
Alarm asserted	Number of times that this sensor has entered the fault state.
Alarm cleared	Number of times that this sensor has left the fault state.

Related commands

show system

show system environment

Command changes

Version 5.5.0-0.1: command added

show system interrupts

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

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

Syntax
```
show system interrupts
```

Mode User Exec and Privileged Exec

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

```
awplus# show system interrupts
```

Output Figure 7-21: Example output from the **show system interrupts** command

```
awplus>show system interrupts
           CPU0
  1:          2   CPM2 SIU  Level Enabled   0     i2c-mpc
  2:        145   CPM2 SIU  Level Enabled   0     spi-mpc
 77:          0   OpenPIC   Level Enabled   0     enet_tx
 78:          2   OpenPIC   Level Enabled   0     enet_rx
 82:          0   OpenPIC   Level Enabled   0     enet_error
 90:       5849   OpenPIC   Level Enabled   0     serial
 91:    2066672   OpenPIC   Level Enabled   0     i2c-mpc
 94:        147   OpenPIC   Level Enabled   0     cpm2_cascade
112:          5   OpenPIC   Edge  Enabled   0     phy_interrupt
114:     398714   OpenPIC   Level Enabled   0     mvPP
115:      26247   OpenPIC   Level Enabled   0     mvPP
119:          0   OpenPIC   Edge  Enabled   0     Power supply status
...
BAD:          0
```

Related commands show system environment

show system mac

Overview This command displays the physical MAC address of the device.

Syntax

```
show system mac
```

Mode User Exec and Privileged Exec

Example To display the physical MAC address enter the following command:

```
awplus# show system mac
```

Output Figure 7-22: Example output from the **show system mac** command

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

show system pci device

Overview Use this command to display the PCI devices on your device.

Syntax

```
show system pci device
```

Mode User Exec and Privileged Exec

Example To display information about the PCI devices on your device, use the command:

```
awplus# show system pci device
```

Output Figure 7-23: Example output from the **show system pci device** command

```
awplus#show system pci device
00:00.0 Class 0600: 14e4:5300 (rev 01)
        Subsystem: 14e4:5300
        Flags: bus master, fast devsel, latency 0, IRQ 5
        Memory at 18000000 (64-bit, non-prefetchable) [size=16K]
        Memory at <unassigned> (64-bit, non-prefetchable) [size=128M]
        Capabilities: [40] Power Management version 3
        Capabilities: [58] #09 [0078]
        Capabilities: [48] Message Signalled Interrupts: 64bit+ Queue=0/0 Enable
-
        Capabilities: [d0] #10 [0041]

00:01.0 Class 0200: 14e4:b321 (rev 12)
        Subsystem: 14e4:4d4c
        Flags: bus master, fast devsel, latency 0, IRQ 5
        Memory at 08000000 (64-bit, non-prefetchable) [size=256K]
        Capabilities: [48] Power Management version 3
        Capabilities: [50] Vital Product Data
        Capabilities: [58] Message Signalled Interrupts: 64bit+ Queue=0/3 Enable
-
        Capabilities: [a0] #11 [0000]
        Capabilities: [ac] #10 [0002]
```

Related commands show system environment

show system pci tree

show system pci tree

Overview Use this command to display the PCI tree on your device.

Syntax

```
show system pci tree
```

Mode User Exec and Privileged Exec

Example To display information about the PCI tree on your device, use the command:

```
awplus# show system pci tree
```

Output Figure 7-24: Example output from the **show system pci tree** command

```
awplus>show system pci tree
-[00]-+-0c.0  11ab:00d1
      \-0d.0  11ab:00d1
```

Related commands

show system environment

show system pci device

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 7-25: 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
```

speed (asyn)

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

Syntax

```
speed <console-speed-in-bps>
```

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

Default The default console speed baud rate is 9600 bps.

Mode Line Configuration

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

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

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

Then log in again to enable the change:

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

Related commands

clear line console

line

show running-config

show startup-config

speed

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.

8 Pluggables and Cabling Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure and monitor Pluggables and Cabling, including:

- Cable Fault Locator for finding faults in copper cabling
- Optical Digital Diagnostic Monitoring (DDM) to help find fiber issues when links go down
- Active Fiber Monitoring for detecting changes in optical power received over fiber cables.

For more information, see the Pluggables and Cabling Feature Overview and Configuration Guide.

Command List

- "clear fiber-monitoring interface" on page 311
- "clear test cable-diagnostics tdr" on page 312
- "debug fiber-monitoring" on page 313
- "fiber-monitoring action" on page 315
- "fiber-monitoring baseline" on page 317
- "fiber-monitoring enable" on page 319
- "fiber-monitoring interval" on page 320
- "fiber-monitoring sensitivity" on page 321
- "show system fiber-monitoring" on page 323
- "show system pluggable" on page 326
- "show system pluggable detail" on page 328
- "show system pluggable diagnostics" on page 331
- "show test cable-diagnostics tdr" on page 333
- "test cable-diagnostics tdr interface" on page 334

clear fiber-monitoring interface

Overview Use this command to clear the Active Fiber Monitoring state of a port. It clears the alarm, baseline and history and starts monitoring from the beginning. It does not change the configuration.

Syntax

```
clear fiber-monitoring interface <port>
```

Parameter	Description
<port>	The name of the port to reset Active Fiber Monitoring on.

Default n/a

Mode Privileged Exec

Usage notes Normally, you do not need to clear the Active Fiber Monitoring state of a port. If the issue resolves itself and the monitored optical power returns to the baseline, the alarm clears automatically.

However, you may need to clear the Active Fiber Monitoring state if the optical power level reduces for a known reason, causing the port to be stuck in the alarm state. In this situation, the alarm will not clear automatically, because Active Fiber Monitoring does not update the baseline when the port is in the alarm state, for security reasons.

Example To clear the Active Fiber Monitoring state for interface port1.0.1, use the command:

```
awplus# clear fiber-monitoring interface port1.0.1
```

Related commands show system fiber-monitoring

Command changes Version 5.4.8-0.2: command added

clear test cable-diagnostics tdr

Overview Use this command to clear the results of the last cable test that was run.

Syntax

```
clear test cable-diagnostics tdr
```

Mode Privileged Exec

Examples To clear the results of a previous cable-diagnostics test use the following commands:

```
awplus# clear test cable-diagnostics tdr
```

Related commands

show test cable-diagnostics tdr

test cable-diagnostics tdr interface

debug fiber-monitoring

Overview Use this command to enable debugging of active fiber monitoring on the specified ports.

Use the **no** variant of this command to disable debugging on all ports or the specified ports.

Syntax

```
debug fiber-monitoring interface <port-list>
no debug fiber-monitoring [interface <port-list>]
```

Parameter	Description
<port-list>	The list of fiber ports to enable or disable debugging for, as a single port, a comma separated list or a hyphenated range.

Default Debugging of active fiber monitoring is disabled by default.

Mode User Exec/Privileged Exec

Usage While debugging is enabled by this command for a port, all the optical power readings for the port are sent to the console.

Example To enable debugging messages for active fiber monitoring of port1.0.1 to be sent to the console, use the commands:

```
awplus# debug fiber-monitoring interface port1.0.1
awplus# terminal monitor
```

To disable debugging messages for active fiber monitoring on port1.0.1, use the command:

```
awplus# no debug fiber-monitoring interface port1.0.1
```

To disable all debugging messages for active fiber monitoring, use the command:

```
awplus# no debug fiber-monitoring
```

Output Figure 8-1: Example output from **debug fiber-monitoring**

```
awplus#debug fiber-monitoring interface port1.0.1
awplus#terminal monitor
% Warning: Console logging enabled
awplus#01:42:50 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1
Reading:1748 Baseline:1708 Threshold:1356
01:42:52 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1717
Baseline:1709 Threshold:1357
01:42:54 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1780
Baseline:1709 Threshold:1357
01:42:56 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1685
Baseline:1710 Threshold:1358
01:42:58 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1701
Baseline:1710 Threshold:1358
01:43:01 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1733
Baseline:1709 Threshold:1357
```

Related commands show system fiber-monitoring

fiber-monitoring action

Overview Use this command to specify an action to be taken if the optical power received on the port changes from the baseline by the amount specified in the **fiber-monitoring sensitivity** command.

Use the **no** variant of this command to remove the specified action or all actions from the port.

Syntax

```
fiber-monitoring action [trap] [shutdown] [continuous]
no fiber-monitoring action [trap|shutdown]
```

Parameter	Description
`trap`	Send an SNMP notification.
`shutdown`	Shutdown the port.
`continuous`	Make the action or actions happen continuously (every polling interval) while the sensor is in the alarm state. Otherwise, the action only happens when the alarm is triggered or cleared.

Default By default a log message is generated, but no additional action is performed.

Mode Interface Configuration mode for a fiber port.

Usage If fiber monitoring is enabled and this command is not used to set an action, a change in received power on a fiber port only generates a log message.

Example To set the device to send an SNMP trap when port1.0.1 or port1.0.4 receive reduced power and when that reduced-power alarm is cleared, use the commands:

```
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# fiber-monitoring action trap
```

To set the device to send an SNMP trap when port1.0.1 or port1.0.4 receive reduced power, and every polling interval after that until the alarm is cleared, use the commands:

```
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# fiber-monitoring action trap continuous
```

To set the device to send an SNMP trap and to shut down the port when port1.0.1 or port1.0.4 receive reduced power, use the commands:

```
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# fiber-monitoring action trap shutdown
```

To set the device to stop shutting down the port if port1.0.1 or port1.0.4 receive reduced power, use the commands:

```
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# no fiber-monitoring action shutdown
```

If the device is set to send an SNMP trap for those ports, it will continue to do so.

To set the device not to perform any action when it receives reduced power on port1.0.1 or port1.0.4, except sending a log message, use the commands:

```
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# no fiber-monitoring action
```

Related commands

fiber-monitoring sensitivity

show system fiber-monitoring

Command changes

Version 5.4.8-0.2: **continuous** parameter added

fiber-monitoring baseline

Overview Use this command to configure how the baseline value for comparison is calculated for active fiber monitoring on the port.

Note that alarm generation will not commence until the link has been up for a full averaging period.

Use the **no** variant of this command to set the fiber-monitoring baseline to its default value.

Syntax

```
fiber-monitoring baseline average <12-150> [interval <2-86400>]
fiber-monitoring baseline fixed <1-65535>
no fiber-monitoring baseline
```

Parameter	Description
`average <12-150>`	Set the baseline optical power received to be based on the moving average of the specified number of most recent (non-zero) values. Default is to use this setting and 12 values.
`interval <2-86400>`	Optionally, specify the optical power polling interval for determining the baseline, in seconds. By default, the baseline polling interval is the same as the monitoring polling interval, which is 5 seconds by default. If specified, this baseline interval should be larger than the monitoring interval. Even if you specify a baseline interval, Active Fiber Monitoring will use the monitoring interval to calculate the initial baseline average. This means the first x baseline readings will be taken at the monitoring interval, where x is the number of readings specified in the **average** parameter. See Usage below for more information.
`fixed <1-65535>`	Set the baseline to a fixed level of received optical power in 0.0001mW. Not recommended—see Usage below.

Default The default is a moving average of the last 12 values, taken at the same interval as the monitoring interval. The monitoring interval is set using the **fiber-monitoring interval** command. If the monitoring interval is set to its default of 5 seconds, the **fiber-monitoring baseline** default will be the average over the last minute.

Mode Interface Configuration for a fiber port

Usage notes There are two ways to configure the baseline. The first is to choose a number of readings to average. This is the default and recommended method. The second is to set a fixed value in units of x0.0001mW.

If a fixed value is required, the easiest way to choose a value is to enable fiber monitoring on the port and use the **show system fiber-monitoring** command to see what readings you can expect.

CAUTION: *We do not recommend setting a fixed value because gradual change over time caused by temperature fluctuations, etc. could lead to unnecessary alarms.*

If you use the averaging method, you can optionally specify how often Active Fiber Monitoring polls the cable to determine the baseline. This allows Active Fiber Monitoring to update the baseline less often than it polls the device for monitoring.

In order to prevent the theoretical possibility of slow clamping, you can set the baseline interval to a large value, so that the baseline average is only updated with the current reading (for example) once per day or once per hour.

As fiber attenuation can be affected by ambient temperature, take care if changing the baseline interval in environments with large daily temperature fluctuations.

Example To set the baseline optical power to a moving average of the last 30 monitoring readings on port1.0.1 and port1.0.4, use the command:

```
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# fiber-monitoring baseline average 30
```

To calculate the baseline based on 12 values taken 24 hours (86400 seconds) apart, instead of using the monitoring interval, use the command:

```
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# fiber-monitoring baseline average 12
interval 86400
```

To set the baseline to its default, averaging the last 12 readings, use the command:

```
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# no fiber-monitoring baseline
```

Related commands

fiber-monitoring interval

fiber-monitoring sensitivity

Command changes Version 5.4.8-0.2: **interval** parameter added

fiber-monitoring enable

Overview Use this command to enable active fiber monitoring on a fiber port. If the port can support fiber monitoring but does not have the correct SFP or fiber type installed, the configuration will be saved, and monitoring will commence when a supported SFP is inserted. Disabling and re-enabling fiber monitoring on a port resets the baseline calculation.

Use the **no** variants of this command to disable active fiber monitoring on the interface, or to remove all the configuration and state for the ports, respectively.

Syntax

```
fiber-monitoring enable
no fiber-monitoring enable
no fiber-monitoring
```

Default Active fiber monitoring is disabled by default.

Mode Interface Configuration mode for a fiber port

Examples To enable active fiber monitoring on port1.0.1 and port1.0.4, use the commands:

```
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# fiber-monitoring enable
```

To disable fiber monitoring on the ports, use the commands:

```
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# no fiber-monitoring enable
```

To remove all fiber-monitoring configuration and state for the ports, use the commands:

```
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# no fiber-monitoring
```

Related commands

fiber-monitoring action

fiber-monitoring sensitivity

show system fiber-monitoring

fiber-monitoring interval

Overview Use this command to configure the fiber monitoring polling interval in seconds for the port. The optical power will be read every <interval> seconds and compared against the calculated threshold values to see if a log message or other action is required.

Use the **no** variant of this command to reset the polling interval to the default (5 seconds).

Syntax

```
fiber-monitoring interval <2-60>
no fiber-monitoring interval
```

Parameter	Description
<2-60>	Optical power polling interval in seconds.

Default The interval is set to 5 seconds by default.

Mode Interface configuration mode for a fiber port.

Example To set the fiber monitoring polling interval for port1.0.1 to 30 seconds, use the commands:

```
awplus(config)# interface port1.0.1
awplus(config-if)# fiber-monitoring interval 30
```

To reset the fiber monitoring polling interval back to the default (5s), use the commands:

```
awplus(config)# interface port1.0.1
awplus(config-if)# no fiber-monitoring interval
```

Related commands fiber-monitoring baseline

show system fiber-monitoring

fiber-monitoring sensitivity

Overview Use this command to configure the sensitivity of the alarm thresholds on the port for active fiber monitoring.

Use the **no** variant of this command to reset the sensitivity to the default.

Syntax

```
fiber-monitoring sensitivity (low|medium|high|highest|fixed
<25-65535>)|relative <0.01-10.0>
```

```
no fiber-monitoring sensitivity
```

Parameter	Description
`low`	Low sensitivity (+/-2 dB)
`medium`	Medium sensitivity (1 dB) (default)
`high`	High sensitivity (the greater of 0.5 dB and 0.0025 mW)
`highest`	The highest sensitivity available: 0.0025mW
`fixed <25-65535>`	Fixed sensitivity at the specified level in 0.0001 mW.
`relative <0.01-10.0>`	Relative sensitivity at the specified level in dB.

Default Medium sensitivity.

Mode User Exec/Privileged Exec

Usage A log message is generated and configured actions are taken if the received optical power drops below the baseline value by the sensitivity configured with this command.

The sensitivity can be configured to one of four pre-defined levels in decibels or to a fixed absolute delta in units of 0.0001mW. The alarm thresholds can be seen in the **show system fiber-monitoring** output. The maximum absolute sensitivity configurable is 0.0025 mW. Note that 0.0025 mW equates to a reduction of approximately 1dB at the maximum attenuation of an AT-SPLX10/1.

Example To set the fiber monitoring sensitivity for port1.0.1 to a relative sensitivity of 0.1 dB, use the commands:

```
awplus(config)# interface port1.0.1
awplus(config-if)# fiber-monitoring sensitivity relative 0.1
```

To reset the fiber monitoring sensitivity to the default (medium), use the commands:

```
awplus(config)# interface port1.0.1
awplus(config-if)# no fiber-monitoring sensitivity
```

Related commands fiber-monitoring action

fiber-monitoring baseline

show system fiber-monitoring

show system fiber-monitoring

Overview Use this command to display settings and current status for Active Fiber Monitoring.

Syntax

```
show system fiber-monitoring
```

Mode User Exec and Privileged Exec

Example To display configuration and status for active fiber monitoring on ports, use the command:

```
awplus# show system fiber-monitoring
```

Output Figure 8-2: Example output from **show system fiber-monitoring**

```
awplus#show sys fiber-monitoring
Fiber Monitoring Status
  Reading units 0.0001mW

Interface port1.0.1
Status:           enabled
Supported:        Supported pluggable
Debugging:        disabled
Interval:         2 seconds
Sensitivity:      1.00dB
Baseline type:    average of last 35 values greater than 50
Status:
 Baseline value:   496
 Alarm threshold:  393
 Alarm:            no
 Last 12 Readings: 498 498 498 498 498 498 498 498 498 498 498 498
 Minimum reading: 486
 Maximum reading: 498

Interface port1.0.4
Status:           enabled
Supported:        Supported pluggable
Debugging:        disabled
Interval:         2 seconds
Sensitivity:      1.00dB
Baseline type:    average of last 30 values greater than 50
Status:
 Baseline value:   0
 Alarm threshold:  0
 Alarm:            no
 Last 12 Readings: 0 0 0 0 0 0 0 0 0 0 0 0
 Minimum reading: 0
 Maximum reading: 0
```

Table 8-1: Parameters in the output from **show system fiber-monitoring**

Parameter	Description
`Reading units`	The units for optical power readings in the rest of the display, e.g. 0.0001mW.
`Status`	Whether active fiber monitoring is enabled or disabled for this port.
`Supported`	Whether the pluggable inserted in this port supports active fiber monitoring.
`Debugging`	Whether debugging of active fiber monitoring is enabled or disabled for this port.
`Interval`	The configured interval between readings of optical power on this port.
`Sensitivity`	The configured sensitivity threshold for optical power changes on this port.
`Baseline type`	How the baseline optical power level is calculated: either the average of the specified number of previous readings or a specified fixed value in 0.0001mW.
`Status`	Current values for the following parameters.
`Baseline value`	The baseline value, calculated according to the configured baseline method, in 0.0001mW.
`Alarm threshold`	The current threshold for a change in optical power, calculated according to the configured sensitivity method, that will result in action.
`Alarm`	Whether the optical power at the most recent reading fallen below the threshold.
`Last 12 readings`	The last 12 optical power values measured, in 0.0001mW, with oldest value first.
`Minimum reading`	The lowest optical power reading since the fiber pluggable was last inserted, or since active fiber monitoring was last enabled on the port.
`Maximum reading`	The highest optical power reading since the fiber pluggable was last inserted, or since active fiber monitoring was last enabled on the port.

Related commands

debug fiber-monitoring

fiber-monitoring action

fiber-monitoring baseline

fiber-monitoring enable

fiber-monitoring interval

fiber-monitoring sensitivity

show system pluggable

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

Syntax

```
show system pluggable [<port-list>]
```

Parameter	Description
<port-list>	The ports to display information about. The port list can be: • a switch port (e.g. port1.0.1) • a continuous range of ports separated by a hyphen (e.g. portport1.0.1-port1.0.4) • a comma-separated list of ports and port ranges (e.g. port1.0.1,port1.0.4)

Mode User Exec and Privileged Exec

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

```
awplus# show system pluggable
```

Output Figure 8-3: Example output from **show system pluggable**

```
awplus#show system pluggable
System Pluggable Information

Port    Vendor           Device          Serial Number    Datecode Type
-------------------------------------------------------------------------------
port1.0.1  ATI              AT-SPSX          A03240R151300867 15032801 1000BASE-SX
port1.0.4  ATI              AT-SPSX          A03240R111800076 15032801 1000BASE-SX
-------------------------------------------------------------------------------
```

Table 9: Parameters in the output from the **show system pluggable** command

Parameter	Description
Port	Specifies the port number for the installed pluggable transceiver.
Vendor	Specifies the vendor's name for the installed pluggable transceiver.
Device	Specifies the device name for the installed pluggable transceiver.

Table 9: Parameters in the output from the **show system pluggable** command

Parameter	Description
`Serial Number`	Specifies the serial number for the installed pluggable transceiver.
`Datecode`	Specifies the manufacturing datecode for the installed pluggable transceiver. Checking the manufacturing datecode with the vendor may be useful when determining Laser Diode aging issues. For more information, see "Troubleshooting Fiber and Pluggable Issues" in the "Pluggables and Cabling" Feature Overview and Configuration Guide.
`Type`	Specifies the device type for the installed pluggable transceiver.

Related commands

show system environment

show system pluggable detail

show system pluggable diagnostics

show system pluggable detail

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

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

Syntax

```
show system pluggable [<port-list>] detail
```

Parameter	Description
<port-list>	The ports to display information about. The port list can be: • a switch port (e.g. port1.0.1) • a continuous range of ports separated by a hyphen (e.g. portport1.0.1-port1.0.4) • a comma-separated list of ports and port ranges (e.g. port1.0.1,port1.0.4)

Mode User Exec and Privileged Exec

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

- **SFP Laser Wavelength**: Specifies the laser wavelength of the installed pluggable transceiver
- **Single mode Fiber**: Specifies the link length supported by the pluggable transceiver using single mode fiber
- **OM1 (62.5µ m) Fiber**: Specifies the link length, in meters (m) or kilometers (km) supported by the pluggable transceiver using 62.5 micron multi-mode fiber.
- **OM2 (50µ m) Fiber**: Specifies the link length (in meters or kilometers) supported by the pluggable transceiver using 50 micron multi-mode fiber.
- **Diagnostic Calibration**: Specifies whether the pluggable transceiver supports DDM or DOM Internal or External Calibration.
  - **Internal** is displayed if the pluggable transceiver supports DDM or DOM Internal Calibration.
  - **External** is displayed if the pluggable transceiver supports DDM or DOM External Calibration.
  - a dash (-) is displayed if neither Internal Calibration or External Calibration is supported.

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

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

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

```
awplus# show system pluggable port1.0.1 detail
```

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

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

Output Figure 8-4: Example output from **show system pluggable detail** for a port

```
awplus#show system pluggable port1.0.1 detail
System Pluggable Information Detail
port1.0.1
==========
Vendor Name:              ATI
Device Name:        AT-SPSX
Device Revision:          A
Device Type:              1000BASE-SX
Serial Number:            A02420N0607J0023
Manufacturing Datecode:   060704
SFP Laser Wavelength:     850nm
Link Length Supported
  Single Mode Fiber :     -
  OM1 (62.5um) Fiber:     150m
  OM2 (50um) Fiber  :     300m
  OM3 (50um) Fiber  :     -
Diagnostic Calibration:   External
Power Monitoring:         Average
```

Table 8-1: Parameters in the output from **show system pluggable detail**

Parameter	Description
Port	Specifies the port the pluggable transceiver is installed in.
Vendor Name	Specifies the vendor's name for the installed pluggable transceiver.
Device Name	Specifies the device name for the installed pluggable transceiver.
Device Revision	Specifies the hardware revision code for the pluggable transceiver. This may be useful for troubleshooting because different devices may support different pluggable transceiver revisions.

Table 8-1: Parameters in the output from **show system pluggable detail** (cont.)

Parameter	Description
`Device Type`	Specifies the device type for the installed pluggable transceiver.
`Serial Number`	Specifies the serial number for the installed pluggable transceiver.
`Manufacturing Datecode`	Specifies the manufacturing datecode for the installed pluggable transceiver. Checking the manufacturing datecode with the vendor may be useful when determining Laser Diode aging issues. For more information, see "Troubleshooting Fiber and Pluggable Issues" in the "Pluggables and Cabling" Feature Overview and Configuration Guide.
`SFP Laser Wavelength`	Specifies the laser wavelength of the installed pluggable transceiver.
`Single Mode Fiber`	Specifies the link length supported by the pluggable transceiver using single mode fiber.
`OM1 (62.5um) Fiber`	Specifies the link length (in µm - micron) supported by the pluggable transceiver using 62.5 micron multi-mode fiber.
`OM2 (50um) Fiber`	Specifies the link length (in µm - micron) supported by the pluggable transceiver using 50 micron multi-mode fiber.
`Diagnostic Calibration`	Specifies whether the pluggable transceiver supports DDM or DOM Internal or External Calibration: **Internal** is displayed if the pluggable transceiver supports DDM or DOM Internal Calibration. **External** is displayed if the pluggable transceiver supports DDM or DOM External Calibration. **-** is displayed if neither Internal Calibration or External Calibration is supported.
`Power Monitoring`	Displays the received power measurement type, which can be either **OMA** (Optical Module Amplitude) or **Avg** (Average Power) measured in µW.

Related commands

show system environment

show system pluggable

show system pluggable diagnostics

show system pluggable diagnostics

Overview This command displays diagnostic information about pluggable transceivers that support Digital Diagnostic Monitoring (DDM).

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

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

Syntax

```
show system pluggable [<port-list>] diagnostics
```

Parameter	Description
<port-list>	The ports to display information about. The port list can be: • a switch port (e.g. port1.0.1) • a continuous range of ports separated by a hyphen (e.g. portport1.0.1-port1.0.4) • a comma-separated list of ports and port ranges (e.g. port1.0.1,port1.0.4)

Mode User Exec and Privileged Exec

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

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

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

Output Figure 8-5: Example output from the **show system pluggable diagnostics** command on a device

```
awplus#show system pluggable diagnostics

System Pluggable Information Diagnostics

port1.0.1           Status              Alarms                    Warnings
                   Reading   Alarm     Max      Min    Warning     Max      Min
Temp: (Degrees C)   44.871       -   100.00   -40.00          -   95.000   -30.00
Vcc: (Volts)        3.3043       -   3.4650   3.1350          -   3.4000   3.2000
Tx Bias: (mA)        3.468       -   13.264    0.000          -   10.264    0.264
Tx Power: (mW)      0.2376       -   0.7943   0.0562          -   0.6310   0.0708
Rx Power: (mW)      0.2104       -   1.0000   0.0126          -   0.7943   0.0200
Rx LOS:              Rx Up

...
```

Table 9: Parameters in the output from the **show system pluggables diagnostics** command

Parameter	Description
Temp (Degrees C)	Shows the temperature inside the transceiver.
Vcc (Volts)	Shows voltage supplied to the transceiver.
Tx Bias (mA)	Shows current to the Laser Diode in the transceiver.
Tx Power (mW)	Shows the amount of light transmitted from the transceiver.
Rx Power (mW)	Shows the amount of light received in the transceiver.
Rx LOS	Rx Loss of Signal. This indicates whether: • light is being received (Rx Up) and therefore the link is up, or • light is not being received (Rx Down) and therefore the link is down

Related commands

show system environment

show system pluggable

show system pluggable detail

show test cable-diagnostics tdr

Overview Use this command to display the results of the last cable-diagnostics test that was run using the TDR (Time Domain Reflectometer) on a fixed copper cable port.

The displayed status of the cable can be either:

- OK
- Open
- Short (within-pair)
- Short (across-pair)
- Error

Syntax

```
show test cable-diagnostics tdr
```

Mode Privileged Exec

Examples To show the results of a cable-diagnostics test use the following command:

```
awplus# show test cable-diagnostics tdr
```

Output Figure 8-6: Example output from the **show test cable-diagnostics tdr** command

```
Port      Pair  Length       Status
-----------------------------------------------
1.0.1     A     -            OK
          B     -            OK
          C     -            OK
          D     -            OK
```

Related commands

clear test cable-diagnostics tdr

test cable-diagnostics tdr interface

test cable-diagnostics tdr interface

Overview Use this command to apply the Cable Fault Locator's cable-diagnostics tests to twisted pair data cables for a selected port. The tests will detect either correct, short circuit, or open, circuit terminations. For more information on running the CFL, see the Pluggables and Cabling Feature Overview and Configuration Guide.

The test can take several seconds to complete. See the related show command to display the test results.

A new test can only be started if no other test is in progress. CFL cannot run on a port that is currently supplying power via PoE.

The displayed status of the cable can be either, OK, Short (within-pair), or Open. The "Open" or "Short" status is accompanied with the distance from the source port to the incorrect termination.

Syntax

```
test cable-diagnostics tdr interface <interface>
```

Parameter	Description
cable-diagnostics	The cable diagnostic tests.
`tdr`	Time Domain Reflectometry.
`interface`	Selects the interface to test.
<interface>	Interface number of the port to be tested, e.g. port1.0.2.

Mode Privileged Exec

Example To run a cable test on the cable inserted into port1.0.1 use the following command:

```
awplus# test cable-diagnostics tdr interface port1.0.1
```

You will receive the following message:

```
Link will go down while test is in progress. Continue? (y/n): y
Select y to continue.
```

```
awplus# y
```

You will then receive the following message:

```
Test started. This will take several seconds to complete. Use
"show test cable-diagnostics tdr" to print results.
```

Related commands

clear test cable-diagnostics tdr

show test cable-diagnostics tdr

9 Connectivity Fault Management Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure Connectivity Fault Management.

For more information, see the Connectivity Fault Management (CFM) Feature Overview and Configuration Guide.

Command List

- "cc interval" on page 337
- "cc multicast" on page 339
- "cc unicast" on page 340
- "clear (MEP Attribute)" on page 341
- "clear ethernet cfm errorlog" on page 342
- "clear mep counter" on page 343
- "ethernet cfm domain-name" on page 344
- "ethernet cfm mep" on page 347
- "mep (FNG attributes)" on page 349
- "mep active" on page 351
- "mep ccm-ltm-priority" on page 353
- "mep crosscheck" on page 355
- "service ma-name" on page 357
- "show ethernet cfm details" on page 360
- "show ethernet cfm domain" on page 365
- "show ethernet cfm errorlog" on page 368
- "show ethernet cfm maintenance-points local mep" on page 370
- "show ethernet cfm maintenance-points remote mep" on page 376

- "show ethernet cfm service" on page 379
- "show mep-alarm status" on page 382

cc interval

Overview Use this command to set the CCM Interval.

Syntax

```
cc ma-name <ma-name> interval <interval>
```

Parameter	Description
`ma-name`	Specify the Maintenance Association for which the Interval is used.
<ma-name>	Specify the Maintenance Association's CLI instance name.
`interval`	Specify the CCM Interval.
<interval>	Specify the CCM Interval (CCI), using one of the following: 1 - CCI of 3 milliseconds (currently not supported) 2 - CCI of 10 milliseconds (currently not supported) 3 - CCI of 100 milliseconds 4 - CCI of 1 second 5 - CCI of 10 seconds 6 - CCI of 1 minute 7 - CCI of 10 minutes.

Default The default interval is 4 (1 second).

Mode Ethernet CFM Configuration

Usage notes Continuity Checks is another term for connectivity fault detection. This makes use of Continuity Check Messages (CCMs) that are periodically sent by an MEP (multicast or unicast) and received by other MEP(s). CCMs can be used to detect connectivity faults across a link (using Link Level MEPs) or across a segment of a VLAN using VLAN aware MEPs, both of which are used within an MD/MA. CCMs are sent periodically at a given rate (or frame interval) that is agreed upon by all the MEPs in the MA. The faster the rate, the more quickly faults can be detected.

If an MEP does not receive a CCM within 3.5 times the expected interval from a peer MEP(s), that MEP declares a connectivity fault. This is known as a “defect”. Upon detecting a defect, the detecting MEP will also set the Remote Defect Indicator (RDI) bit for its outgoing CCM messages to its peer MEP(s) so as to notify the peer MEPs that a defect has been detected. If the defect persists long enough (generally 2.5 seconds), then an “alarm” is declared. If an alarm is declared, then the defect has to abate long enough (generally 10 seconds) for the alarm to clear.

Example To set the CCM interval of a Maintenance Association named “MA-INST2-1” to the value of “4”, use the commands:

```
awplus(config)# ethernet cfm domain-name MD-INST2
awplus(config-ether-cfm)# cc ma-name MA-INST2-1 interval 4
```

Related commands ethernet cfm domain-name

service ma-name

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

cc multicast

Overview Use this command to enable a Local MEP to send CCMs using multicast, or to disable sending CCMs altogether.

Syntax

```
cc multicast state {enable|disable}
```

Parameter	Description
`state`	Specify to either enable or disable CFM multicast CCMs.
`enable`	Start sending periodic multicast frames.
`disable`	Stop sending multicast frames.

Default Multicast is disabled by default.

Mode Interface Ethernet CFM MEP Configuration

Usage notes Continuity Checks is another term for connectivity fault detection. This makes use of Continuity Check Messages (CCMs) that are periodically sent by an MEP (multicast or unicast) and received by other MEP(s). CCMs can be used to detect connectivity faults across a link (using Link Level MEPs) or across a segment of a VLAN using VLAN aware MEPs, both of which are used within an MD/MA. CCMs are sent using multicast or unicast (but not both).

In order to enable a Local MEP to send, the Local MEP's "active" administrative state must be set to true, using the command mep active.

Example To configure a Local MEP to send CCMs using multicast, use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# ethernet cfm mep down mpid 12 domain-name
MD-INST2 ma-name MA-INST2-1
awplus(config-if-eth-cfm-mep)# cc multicast state enable
```

Related commands

ethernet cfm domain-name

ethernet cfm mep

service ma-name

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

cc unicast

Overview Use this command to enable a Local MEP to send CCMs using unicast, or to disable sending CCMs altogether.

Syntax

```
cc unicast rmpid <rmep-id> state {enable|disable}
```

Parameter	Description
`rmpid`	The remote MEP that the Local MEP is to unicast to.
`<rmep-id>`	The remote MEP ID in the range 1-8191.

Mode Interface Ethernet CFM MEP Configuration

Usage notes Continuity Checks is another term for connectivity fault detection. This makes use of Continuity Check Messages (CCMs) that are periodically sent by an MEP (multicast or unicast) and received by other MEP(s). CCMs can be used to detect connectivity faults across a link (using Link Level MEPs) or across a segment of a VLAN using VLAN aware MEPs, both of which are used within an MD/MA. CCMs are sent using multicast or unicast (but not both).

In order to enable a Local MEP to send, the Local MEP's "active" administrative state must be set to true, using the command mep active.

In order to send unicast CCMs, the Remote MEP has to be configured along with its MAC address.

Example To configure a Local MEP to send CCMs using unicast, use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# ethernet cfm mep down mpid 12 domain-name
MD-INST2 ma-name MA-INST2-1
awplus(config-if-eth-cfm-mep)# cc unicast rmpid 21 state enable
```

Related commands

ethernet cfm domain-name

ethernet cfm mep

mep crosscheck

service ma-name

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

clear (MEP Attribute)

Overview Use this command to clear a Local MEP attribute.

Syntax

```
clear {ccm-ltm-priority|lowest-priority-defect|fng-alarm-time
|reset-fng-time|active|all}
```

Parameter	Description
`ccm-ltm-priority`	Set the queuing and p-bit priority for CCM messages to their default value of 7.
`lowest-priority-defect`	Set the Fault Notification Generation (FNG) lowest alarm priority defect to the default value of 2.
`fng-alarm-time`	Set the Fault Notification Generation (FNG) time for a defect to be present before an alarm is raised to the default value of 2.5 seconds.
`reset-fng-time`	Set the Fault Notification Generation (FNG) time for a defect to abate before an alarm is cleared to the default value of 10 seconds.
`active`	Set the Local MEP's Active state to the default value of False, which sets the Local MEP's Administrative State to Down.
`all`	Set all of the above attributes to their default values.

Mode Interface Ethernet CFM MEP Configuration

Example To set the active state of the Local MEP to False, use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# ethernet cfm mep down mpid 12 domain-name
MD-INST2 ma-name MA-INST2-1
awplus(config-if-eth-cfm-mep)# clear active
```

Related commands

ethernet cfm domain-name

ethernet cfm mep

mep (FNG attributes)

service ma-name

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

clear ethernet cfm errorlog

Overview Use this command to clear the Event List for all Maintenance Associations (MAs) associated with the specified Maintenance Domain (MD).

Syntax

```
clear ethernet cfm errorlog domain <domain-name>
```

Parameter	Description
<domain-name>	Specify the domain name

Mode Privileged Exec

Usage notes When a new error is detected for an MA that is associated with an MD, and the error is due to an error from a received or missing CCM from a Remote MEP, an event is logged to the CFM Errors Event List.

Example To clear the event list for all MA's associated with an MD named "MD-INST2", use the command:

```
awplus# clear ethernet cfm errorlog domain MD-INST2
```

Related commands show ethernet cfm errorlog

Command changes Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

clear mep counter

Overview Use this command to clear statistics counters for all Local MEPs within a given Maintenance Association (MA) and its associated Maintenance Domain (MD), or to optionally clear counters for one specific Local MEP.

Syntax

```
clear mep counter domain <domain-name> service <ma-name>
[mep <mep-id>]
```

Parameter	Description
`domain`	Specify the Maintenance Domain that Local MEP(s) are to have their counters cleared for. Both domain and service must be specified.
`<domain-name>`	Specify the Maintenance Domain's CLI instance name.
`service`	Specify the Maintenance Association that the Local MEP(s) are to have their counters cleared for. Both domain and service must be specified.
`<ma-name>`	Specify the CLI name that identifies the service (Maintenance Association (MA)) instance.
`mep`	Specify one specific Local MEP.
`<mep-id>`	Specify the Local MEP instance by MEP-id.

Mode User Exec/Privileged Exec

Example To clear the statistic counter for an MEP with the MEP ID "12", use the command:

```
awplus# clear mep counter domain MD-INST1 service MA-INST1-1 mep
12
```

Related commands show ethernet cfm maintenance-points local mep

Command changes Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

ethernet cfm domain-name

Overview Use this command to create and configure a CFM Maintenance Domain, or to enter Ethernet CFM Configuration mode for an existing Maintenance Domain instance.

Use the **no** variant of this command to destroy the Maintenance Domain's instance that was previously created.

Syntax

```
ethernet cfm domain-name <domain-name>
```

```
ethernet cfm domain-name <domain-name> md-type character-string
md-type-name <md-type-name> level <level> [mip-creation none]
```

```
ethernet cfm domain-name <domain-name> md-type dns-based
md-type-name <md-type-name> level <level> [mip-creation none]
```

```
ethernet cfm domain-name <domain-name> md-type mac md-type-name
<md-type-name> level <level> [mip-creation none]
```

```
ethernet cfm domain-name <domain-name> md-type no-name level
<level> [mip-creation none]
```

```
no ethernet cfm domain-name <domain-name>
```

Parameter	Description
<domain-name>	The name that identifies this Maintenance Domain instance. If creating this instance, specify the remaining parameters. If re-entering configuration mode for this instance, use this parameter to identify this instance, and do not enter the remaining parameters.
md-type	Specify the name type. The MD name part of the MAID field may or may not appear in the CCM message. There are different formats and conventions for the name depending on type.
character-string	Specify the md-type as Character String-based MD name format. The <md-type-name> is a character string of 1 to 43 characters. This character string plus the Short MA name that is configured for an MA make up the MAID field in a CCM message.
md-type-name	The Maintenance Domain type.
<md-type-name>	The value of the MD type name, which depends on the md-type selected.
dns-based	Specify the md-type as DNS-based MD name format. The <md-type-name> is a Domain Name like string of 1 to 43 characters. This is a globally unique text string derived from a DNS name. This DNS based string plus the Short MA name that is configured for an MA make up the MAID field in a CCM message.

Parameter	Description
`mac`	Specify the md-type as MAC-based MD name format. The <md-type-name> consists of a MAC address + 2-octet (unsigned) integer in the form of HHHH.HHHH.HHHH:<2-octet integer>. This MAC based string plus the Short MA name that is configured for an MA make up the MAID field in a CCM message.
`no-name`	Specify the md-type whereby no MD name is to appear in the CCM message.
`level`	Specify the Level the Domain operates in.
`<level>`	0 to 7.
`mip-creation`	Optional parameter that specifies the MIP creation permission value.
`none`	Specifies that no MIPs are to be created (default and only choice).

Mode Global Configuration

Usage notes A Maintenance Domain is a Connectivity Fault Management (CFM) term that represents the administrative area of a network from which an operator can manage VLANs that traverse their area. An MD can also be scoped to a simple Ethernet link. To differentiate different administrative areas, an MD is made up of a name and a level. As part of CFM, a Connectivity Check Message (CCM) is used to detect Ethernet connectivity faults amongst nodes that participate in CFM. CCM messages carry the MD name within the MAID field as well as carries the level of the MD.

This command is used to configure the MD name, which can be chosen from a variety of name format types, as well as the level.

Example To create a Maintenance Domain instance named “MD-INST2” with a character string-based name of “MD-12L3” and a level of 3, use the command:

```
awplus(config)# ethernet cfm domain-name MD-INST2 md-type
character-string md-type-name MD-12L3 level 3
```

To enter Ethernet CFM Configuration mode for an existing MD instance named “MD-INST2”, use the command:

```
awplus(config)# ethernet cfm domain-name MD-INST2
awplus(config-ether-cfm)#
```

To destroy a Maintenance Domain instance named “MD-INST2”, use the command:

```
awplus(config)# no ethernet cfm domain-name MD-INST2
```

Related commands cc interval

cc multicast

cc unicast

cfm-sf-notify

clear (MEP Attribute)

ethernet cfm mep

mep (FNG attributes)

mep crosscheck

service ma-name

show ethernet cfm domain

show ethernet cfm errorlog

show ethernet cfm maintenance-points remote mep

show ethernet cfm service

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

ethernet cfm mep

Overview Use this command to create a Local MEP instance, or to enter Interface Ethernet CFM MEP Configuration mode for an existing Local MEP's instance, so you can configure it.

Use the **no** variant of this command to destroy the Local MEP instance.

Syntax

```
ethernet cfm mep down mpid <mep-id> domain-name <domain-name>
ma-name <ma-name>
```

```
no ethernet cfm mep down mpid <mep-id> domain-name <domain-name>
ma-name <ma-name>
```

Parameter	Description
`down`	Specify the Local MEP as a Down MEP.
`mpid`	Specify the Local MEP ID.
`<mep-id>`	1-8191. This must be unique ID for all MEPs in the MA (both local and remote).
`domain-name`	Specify the Maintenance Domain that the Local MEP is to be associated with.
`<domain-name>`	Specify the Maintenance Domain's CLI instance name.
`ma-name`	Specify the Maintenance Association that the Local MEP is to be associated with.
`<ma-name>`	Specify the Maintenance Association's CLI instance name.

Mode Interface Configuration

Usage notes Maintenance Points are entities that exist within an MD/MA and can perform the CFM/802.1ag functions such as Continuity Checks for fault management. The main type of MP is a Maintenance End Point (MEP). This type of maintenance point sits at the edges of a Maintenance Domain but is a member of only one MA within the Maintenance Domain. Thus an MEP is used at the end of a VLAN segment, or it is used at the end of a link. MPs live on bridge ports and station ports. On a bridge port, there are two types.

- An Up Maintenance Entity is considered an inward MP. It communicates across the inside of the bridge to the other side, and this allows it to reach the outside world. It lives on a bridge port for a given VLAN, but it does not use this port to send or receive to get to the outside world. Instead, it sends and receives through the inside of the bridge and communicates to the outside world through the other VLAN port members. An Up MP cannot be used for Link Level CFM.
- A Down Maintenance Entity is considered an outward MP. It sends and receives only through its bridge port outwardly to the outside world, and does not communicate inside the bridge. A Down MP is not subject to blocking due to Spanning Tree Protocol (STP) or any other protocol trying to

prevent loops in the network. As such, it is important that Down MPs be used in an MD/MA that is not subject to topology loops. A Down MP can be VLAN aware or link-local.

An MEP can be either Up or Down for a given MD/MA, but within a bridge for the same MD/MA, there can only be one Up or Down MEP (not both). An Up MEP must be VLAN aware. A Down MEP may be VLAN aware. Otherwise, a Down MEP is allowed to be link local (VLAN unaware), and its scope is that of the entire link.

AlliedWare Plus supports Down Maintenance Entities only.

Example To create a local MEP instance context with a domain name of "MD-INST2" and an MA name of "MA-INST2-1", use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# ethernet cfm mep down mpid 12 domain-name
MD-INST2 ma-name MA-INST2-1
```

To re-enter a local MEP instance context with the domain name "MD-INST2" and the MA name "MA-INST2-1", use the commands:

```
awplus(config-if)# ethernet cfm mep down mpid 12 domain-name
MD-INST2 ma-name MA-INST2-1
awplus(config-if-eth-cfm-mep)#
```

To destroy a local MEP instance context with the domain name "MD-INST2" and the MA name "MA-INST2-1", use the commands:

```
awplus(config-if)# no ethernet cfm mep down mpid 12 domain-name
MD-INST2 ma-name MA-INST2-1
```

Related commands

cc multicast

cc unicast

cfm-sf-notify

clear (MEP Attribute)

ethernet cfm domain-name

mep (FNG attributes)

mep crosscheck

service ma-name

show ethernet cfm errorlog

show ethernet cfm maintenance-points remote mep

show ethernet cfm service

show mep-alarm status

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

mep (FNG attributes)

Overview Use this command to configure the Fault Notification Generation (FNG) attributes of a Local MEP.

Syntax

```
mep {lowest-priority-defect <defect-priority>|
fng-alarm-time <soak-time>|reset-fng-time <abate-time>}
```

Parameter	Description
`lowest-priority-defect <defect-priority>`	The lowest level defect allowed to generate alarms. An integer in the range 1 to 6. T he default is 2.
`fng-alarm-time <soak-time>`	The time that the defects must be present before an alarm is generated. An integer in the range of 250 to 1000 in increments of 10 ms. The default is 250 (2.5 seconds).
`reset-fng-time <abate-time>`	The time that the defect must be absent before the alarm is cleared. An integer in the range of 250 to 1000 in increments of 10 ms. The default is 1000 (10 seconds).

Mode Interface Ethernet CFM MEP Configuration

Usage notes Maintenance Points are entities that exist within an MD/MA and can perform the CFM/802.1ag functions such as Continuity Checks for fault management. The main type of MP is a Maintenance End Point (MEP). This type of maintenance point sits at the edges of a Maintenance Domain but is a member of only one MA within the Maintenance Domain. Thus an MEP is used at the end of a VLAN segment, or it is used at the end of a link.

A Local MEP can detect defects in connectivity of a VLAN or a local link using Continuity Check Messages (CCM) by sending and receiving CCMs with Remote MEP peers. Any defects detected locally can also be conveyed to Remote MEP peers by sending a Remote Defect Indicator (RDI) to the peers within a Continuity Check Message (CCM). If defects persist long enough, an alarm can be generated.

Use this command to configure the following attributes of a Local MEP:

- Fault Notification Generation Lowest Alarm Priority Defect — the lowest defect priority that can cause an alarm to be raised. This configuration parameter specifies the lowest defect that has to occur before an alarm can be generated. Any priority less than this will not result in an alarm notification. Note that if a local defect is detected and its priority is not high enough to generate an alarm, then the Local MEP will not send an RDI to its Remote MEP peers, which is used to notify the peers of a connectivity fault. We recommend you keep the lowest alarm priority defect set to 2.
- Fault Notification Generation Alarm timers — the timers that determine whether a defect has been present long enough to result in an alarm being generated, or whether a defect has been abated for long enough to clear an alarm.

Example

To clear an alarm after the defect has been abated for 6 seconds, use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# ethernet cfm mep down mpid 12 domain-name
MD-INST2 ma-name MA-INST2-1
awplus(config-if-eth-cfm-mep)# mep reset-fng-time 600
```

Related commands

clear (MEP Attribute)

ethernet cfm domain-name

ethernet cfm mep

service ma-name

show mep-alarm status

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

mep active

Overview Use this command to specify the administrative state of the Local MEP.

Syntax

```
mep active {true|false}
```

Parameter	Description
`true`	Put the Local MEP into a state of active, which enables it to perform various functions such as processing CCM messages.
`false`	Specify the state of the Local MEP to cease functioning.

Default false

Mode Interface Ethernet CFM MEP Configuration

Usage notes Maintenance Points are entities that exist within an MD/MA and can perform the CFM/802.1ag functions such as Continuity Checks for fault management. The main type of MP is a Maintenance End Point (MEP). This type of maintenance point sits at the edges of a Maintenance Domain but is a member of only one MA within the Maintenance Domain. Thus an MEP is used at the end of a VLAN segment, or it is used at the end of a link.

A Local MEP can detect defects in connectivity of a VLAN or a local link using Continuity Check Messages (CCM) by sending and receiving CCMs with Remote MEP peers. Any defects detected locally can also be conveyed to Remote MEP peers by sending a Remote Defect Indicator (RDI) to the peers within a Continuity Check Message (CCM). If defects persist long enough, an alarm can be generated.

Setting the Local MEP's Administrative State to true enables it to perform various functions such as processing CCM messages. Setting the state to false deactivates the Local MEP.

Example To set the administrative state of the local MEP to “active”, use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# ethernet cfm mep down mpid 12 domain-name
MD-INST2 ma-name MA-INST2-1
awplus(config-if-eth-cfm-mep)# mep active true
```

Related commands

clear (MEP Attribute)

ethernet cfm domain-name

ethernet cfm mep

service ma-name

show mep-alarm status

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

mep ccm-ltm-priority

Overview Use this command to specify the queuing and p-bit priority for CCM messages.

Syntax

```
mep ccm-ltm-priority <0-7>
```

Parameter	Description
<0-7>	The queuing and p-bit priority for CCM messages.

Default 7

Mode Interface Ethernet CFM MEP Configuration

Usage notes Maintenance Points are entities that exist within an MD/MA and can perform the CFM/802.1ag functions such as Continuity Checks for fault management. The main type of MP is a Maintenance End Point (MEP). This type of maintenance point sits at the edges of a Maintenance Domain but is a member of only one MA within the Maintenance Domain. Thus an MEP is used at the end of a VLAN segment, or it is used at the end of a link.

A Local MEP can detect defects in connectivity of a VLAN or a local link using Continuity Check Messages (CCM) by sending and receiving CCMs with Remote MEP peers. CCMs are high priority messages by default, but the priority is configurable, although we do not recommend changing it. Any defects detected locally can also be conveyed to Remote MEP peers by sending a Remote Defect Indicator (RDI) to the peers within a Continuity Check Message (CCM). If defects persist long enough, an alarm can be generated.

Example To set the queuing and p-bit priority for CCM messages to 6, use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# ethernet cfm mep down mpid 12 domain-name
MD-INST2 ma-name MA-INST2-1
awplus(config-if-eth-cfm-mep)# mep ccm-ltm-priority 6
```

CCMs should be the highest priority message so we recommend leaving their priority as 7.

Related commands

clear (MEP Attribute)

ethernet cfm domain-name

ethernet cfm mep

service ma-name

show mep-alarm status

Command changes Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

mep crosscheck

Overview Use this command within the MD instance context to create a Remote MEP instance and configure its parameters.

Use the **no** variant of this command to destroy the Remote MEP instance.

Syntax

```
mep crosscheck mpid <rmep-id> ma-name <ma-name> [mac
<HHHH.HHHH.HHHH>]
```

```
no mep crosscheck mpid <rmep-id> ma-name <ma-name>
```

Parameter	Description
`mpid`	Specify the Remote MEP id.
`<rmep-id>`	1-8191. This must be unique ID for all MEPs in the MA (both local and remote).
`ma-name`	Specify the Maintenance Association that the Remote MEP is to be associated with.
`<ma-name>`	Specify the Maintenance Association's CLI instance name.
`mac`	Optionally, when using unicast for communication between a Local MEP and a Remote MEP, specify the remote MEP's MAC address.
`<HHHH.HHHH.HHHH>`	Specify the Remote MEP's MAC address using the HHHH.HHHH.HHHH format where H is a hexadecimal value.

Mode Ethernet CFM Configuration

Usage notes Maintenance Points are entities that exist within an MD/MA and can perform the CFM/802.1ag functions such as Continuity Checks for fault management. The main type of MP is a Maintenance End Point (MEP). This type of maintenance point sits at the edges of a Maintenance Domain but is a member of only one MA within the Maintenance Domain. Thus an MEP is used at the end of a VLAN segment, or it is used at the end of a link. MPs live on bridge ports and station ports. On a bridge port, there are two types.

- An Up Maintenance Entity is considered an inward MP. It communicates across the inside of the bridge to the other side, and this allows it to reach the outside world. It lives on a bridge port for a given VLAN, but it does not use this port to send or receive to get to the outside world. Instead, it sends and receives through the inside of the bridge and communicates to the outside world through the other VLAN port members. An Up MP cannot be used for Link Level CFM.
- A Down Maintenance Entity is considered an outward MP. It sends and receives only through its bridge port outwardly to the outside world, and does not communicate inside the bridge. A Down MP is not subject to blocking due to Spanning Tree Protocol (STP) or any other protocol trying to prevent loops in the network. As such, it is important that Down MPs be used

in an MD/MA that is not subject to topology loops. A Down MP can be VLAN aware or link-local.

An MEP can be either Up or Down for a given MD/MA, but within a bridge for the same MD/MA, there can only be one Up or Down MEP (not both). An Up MEP must be VLAN aware. A Down MEP may be VLAN aware. Otherwise, a Down MEP is allowed to be link local (VLAN unaware), and its scope is that of the entire link.

Example To create a remote MEP instance named "MA-INST2-1" with an MEP ID of 21, use the command:

```
awplus(config-ether-cfm)# mep crosscheck mpid 21 ma-name
MA-INST2-1
```

To destroy the remote MEP instance named "MA-INST2-1" with the MEP ID of 21, use the command:

```
awplus(config-ether-cfm)# no mep crosscheck mpid 21 ma-name
MA-INST2-1
```

Related commands

cc unicast

ethernet cfm domain-name

ethernet cfm mep

service ma-name

show ethernet cfm errorlog

show ethernet cfm maintenance-points remote mep

show ethernet cfm service

show mep-alarm status

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

service ma-name

Overview Use this command to create a Maintenance Association instance within the MD instance context and configure its parameters.

Use the **no** variant of this command to destroy the Maintenance Association instance.

Syntax

```
service ma-name <ma-name> ma-type
{icc|integer|primary-vid|string|vpn-id} ma-type-name
<ma-type-name> [vlan <primary-vid> [mip-creation {none}]]

no service <ma-name>
```

Parameter	Description
<ma-name>	The CLI name that identifies this Maintenance Association (MA) instance.
ma-type	Specify the MA name type. The MA name part of the MAID field appears in the CCM message. There are different formats and conventions for the name depending on the type.
icc	Specify the ma-type as ICC based MA name format. The <ma-type-name> is a 13 byte character string consisting of a 1 to 6 character ITU Carrier Code (ICC) plus a 1 to 6 character Unique MEGID (UMC) code for the name. Any remaining characters are padding out with NULLs by the system to fill out the 13 bytes. This can only be used with Maintenance Domain whose name md-type is set to “No name”.
integer	Specify the ma-type as Integer based MA name format. The <ma-type-name> Is a number up to 2 Bytes (0..65535).
primary-vid	Specify the ma-type as Primary VLAN-id based MA name format. The <ma-type-name> Is the VLAN id number that has been assigned to the MA as the primary VLAN.
string	Specify the ma-type as Character String based MA name format. The <ma-type-name> is a string of 1 to 45 characters.
vpn-id	Specify the ma-type as an RFC2685 VPN ID based MA name format. The <ma-type-name> is a 7 Byte value divided into two parts. The first part makes up the VPN's OUI which is three octets and the remaining four octets make up the VPN Index. The format is HHHHHH.HHHHHHHH where H is a hexadecimal digit.
ma-type-name	The Maintenance Association (MA) name type.
<ma-type-name>	The value of the MA type name, which depends on the ma-type selected (icc, integer, primary-vid, string, vpn-id).
vlan	An optional parameter that specifies the VLAN.
<primvary-vid>	Specify the ID of the primary VLAN in the MA.

Parameter	Description
`mip-creation`	Optional parameter that specifies the MIP creation permission value.
`none`	Specifies that no MIPs are to be created (the default and only choice).

Mode Ethernet CFM Configuration

Usage notes A Maintenance Association is a Connectivity Fault Management (CFM) term that represents a particular segment of a network within a Maintenance Domain. An MA can represent a segment of a VLAN that is managed for connectivity within that segment. As a VLAN is often the granularity that a Network Service Provider sells to their customer, an MA is often referred to as a "Service". An MA can also be used to represent a link and in this case the MA is VLAN unaware.

As part of CFM, a Connectivity Check Message (CCM) is used to detect Ethernet connectivity faults amongst nodes that participate in CFM. CCM messages carry the MA name within the MAID field. Within an MD instance context, this command is used to configure the MA name, which can be chosen from a variety of format types.

Example To create a Maintenance Association instance named "MA-INST2-1" with an MA name type of "string" and value of "MA-12V100", use the command:

```
awplus(config-ether-cfm)# service ma-name MA-INST2-1 ma-type
string ma-type-name MA-12V100
```

To destroy a Maintenance Association instance named "MA-INST2-1", use the command:

```
awplus(config-ether-cfm)# no service MA-INST2-1
```

Related commands

cc interval

cc multicast

cc unicast

cfm-sf-notify

clear (MEP Attribute)

ethernet cfm domain-name

ethernet cfm mep

mep (FNG attributes)

mep crosscheck

show ethernet cfm domain

show ethernet cfm errorlog

show ethernet cfm maintenance-points remote mep

show ethernet cfm service

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show ethernet cfm details

Overview Use this command to show CFM configuration, status, and statistics in detail for all CFM entities that the system knows about.

Syntax

```
show ethernet cfm details
```

Mode User Exec/Privileged Exec

Example To show CFM configuration, status, and statistics in detail for all CFM entities, use the command:

```
awplus# show ethernet cfm details
```

The output loops through the hierarchy of MDs, then MAs within each MD, then local MEPs within that MA, and finally remote MEPs within that MA.

Output Figure 9-1: Example output from **show ethernet cfm details**

```
awplus#show ethernet cfm details

=========================================================
Maintenance Domain
=========================================================
Maintenance Domain Name........... MD-INST1
Maintenance Domain Name Format.... character-string
Maintenance Domain Name Value..... MD-12L3
Level............................. 3
Associated CFM Services........... (VLAN   400 ): MA-INST1-1
                                   (VLAN   300 ): MA-INST1-2
MIP Creation...................... None

Service
-------
CFM Service Name.................. MA-INST1-1
CFM Domain Name................... MD-INST1
CFM Domain Level.................. 3
Primary VLAN...................... 400
Maintenance Assoc Name Format..... string
Maintenance Assoc Name Value...... MA-12V400
CCM Transmission Interval......... 1 second
Local MEPs........................ MEP DOWN
                                   2 (interface port1.0.3)
Configured Remote MEPs............ 102
Missing Remote MEPs............... None
Current MEP Defects............... -
MIP Creation...................... None
```

```
Local Maintenance End Point
---------------------------
Domain Name..................... MD-INST1
MA Service Name................. MA-INST1-1
MA Primary VLAN................. 400
MEP ID.......................... 2
Direction....................... Down
Interface....................... port1.0.3
    MEP Active State............ True
    CC State.................... Enabled
    CC Type..................... Multicast
    PDU VLAN Priority........... 7
    MAC-address................. eccd.6dc9.bef6
    Tx-RDI...................... False
    Current Defects............. -
    Current Highest Defect Alarm.. -
    Alarm Minimum Defect........ 2 (someMACstatusDefect)
    Alarm Trip Time............. AUTO (2.5 seconds)
    Alarm Reset Time............ AUTO (10 seconds)
    Configured Remote MEPs...... 102
    Missing Remote MEPs......... None
    Error CCM Reason............ N/A
    Last Error CCM.............. N/A
    Cross-connect Defect Reason... N/A
    Last Cross Connect CCM...... N/A
Counters
Domain Name..................... MD-INST1
MA Service Name................. MA-INST1-1
MA Service VLAN................. 400
MEP ID.......................... 2
Direction....................... DOWN
Interface....................... port1.0.3
   Tx CCM Count................. 0
   Rx Out-of-Sequence CCM..... 0

Remote Maintenance End Point
----------------------------
CFM Service Name................ MA-INST1-1
CFM Domain Name................. MD-INST1
Remote MEPID.................... 102
Receiving CCMs.................. Wait
Rx RDI.......................... -
MAC Address..................... -
Port Status..................... -
Interface Status................ -
```

```
Service
-------
CFM Service Name.................. MA-INST1-2
CFM Domain Name................... MD-INST1
CFM Domain Level.................. 3
Primary VLAN...................... 300
Maintenance Assoc Name Format..... string
Maintenance Assoc Name Value...... MA-12V300
CCM Transmission Interval......... 1 second
Local MEPs........................ MEP DOWN
                                   1 (interface port1.0.1)
                                   MEP DOWN
                                   200 (interface port1.0.2)
Configured Remote MEPs............ 101,1001
Missing Remote MEPs............... 101,1001
Current MEP Defects............... 3 (someRMEPCCMdefect)
MIP Creation...................... None

Local Maintenance End Point
---------------------------
Domain Name....................... MD-INST1
MA Service Name................... MA-INST1-2
MA Primary VLAN................... 300
MEP ID............................ 1
Direction......................... Down
Interface......................... port1.0.1
    MEP Active State.............. True
    CC State...................... Enabled
    CC Type....................... Multicast
    PDU VLAN Priority............. 7
    MAC-address................... eccd.6dc9.bef6
    Tx-RDI........................ True
    Current Defects............... 3 (someRMEPCCMdefect)
    Current Highest Defect Alarm.. 4 (someRMEPCCMdefect)
    Alarm Minimum Defect.......... 2 (someMACstatusDefect)
    Alarm Trip Time............... AUTO (2.5 seconds)
    Alarm Reset Time.............. AUTO (10 seconds)
    Configured Remote MEPs........ 101,1001
    Missing Remote MEPs........... 101,1001
    Error CCM Reason.............. N/A
    Last Error CCM................ N/A
    Cross-connect Defect Reason... N/A
    Last Cross Connect CCM........ N/A
Counters
Domain Name....................... MD-INST1
MA Service Name................... MA-INST1-2
MA Service VLAN................... 300
MEP ID............................ 1
Direction......................... DOWN
Interface......................... port1.0.1
   Tx CCM Count................... 121
   Rx Out-of-Sequence CCM......... 0
```

```
Local Maintenance End Point
---------------------------
Domain Name..................... MD-INST1
MA Service Name................. MA-INST1-2
MA Primary VLAN................. 300
MEP ID.......................... 200
Direction....................... Down
Interface....................... port1.0.2
    MEP Active State............ True
    CC State.................... Enabled
    CC Type..................... Multicast
    PDU VLAN Priority........... 7
    MAC-address................. eccd.6dc9.bef6
    Tx-RDI...................... True
    Current Defects............. 3 (someRMEPCCMdefect)
    Current Highest Defect Alarm.. 4 (someRMEPCCMdefect)
    Alarm Minimum Defect........ 2 (someMACstatusDefect)
    Alarm Trip Time............. AUTO (2.5 seconds)
    Alarm Reset Time............ AUTO (10 seconds)
    Configured Remote MEPs...... 101,1001
    Missing Remote MEPs......... 101,1001
    Error CCM Reason............ N/A
    Last Error CCM.............. N/A
    Cross-connect Defect Reason... N/A
    Last Cross Connect CCM...... N/A
Counters
Domain Name..................... MD-INST1
MA Service Name................. MA-INST1-2
MA Service VLAN................. 300
MEP ID.......................... 200
Direction....................... DOWN
Interface....................... port1.0.2
   Tx CCM Count................. 0
   Rx Out-of-Sequence CCM....... 0

Remote Maintenance End Point
----------------------------
CFM Service Name................ MA-INST1-2
CFM Domain Name................. MD-INST1
Remote MEPID.................... 101
Receiving CCMs.................. Fail
Rx RDI.......................... -
MAC Address..................... -
Port Status..................... -
Interface Status................ -

Remote Maintenance End Point
----------------------------
CFM Service Name................ MA-INST1-2
CFM Domain Name................. MD-INST1
Remote MEPID.................... 1001
Receiving CCMs.................. Fail
Rx RDI.......................... -
MAC Address..................... -
Port Status..................... -
Interface Status................ -
```

Related commands

show ethernet cfm domain

show ethernet cfm maintenance-points local mep

show ethernet cfm maintenance-points remote mep

show ethernet cfm service

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show ethernet cfm domain

Overview Use this command to show the Ethernet CFM Domain(s) that have been configured in summary format. Options include the ability to show all domains with detailed information, or to show a specified domain with detailed information.

Syntax

```
show ethernet cfm domain
show ethernet cfm domain details
show ethernet cfm domain <domain-name> details
```

Parameter	Description
<domain-name>	The CLI name that identifies this Maintenance Domain instance.
details	Provide detailed information in the output.

Mode Privileged Exec

Example To show all domain configurations in summary format, use the command:

```
awplus# show ethernet cfm domain
```

To show all domains in detail, use the command:

```
awplus# show ethernet cfm domain details
```

To show a specific domain named "MD-INST1" in detail, use the command:

```
awplus# show ethernet cfm domain MD-INST1 details
```

Output Figure 9-2: Example output from **show ethernet cfm domain**

```
awplus#show ethernet cfm domain

CFM Domain Name                    Level
---------------------------------------
MD-INST1                           0
MD-INST2                           3
```

Table 9-1: Parameters in the output from **show ethernet cfm domain**

Parameter	Description
CFM Domain Name	The Maintenance Domain name for the managed object.
Level	The level for the domain.

Figure 9-3: Example output from **show ethernet cfm domain details**

```
awplus#show ethernet cfm domain details

Maintenance Domain Name..... MD-INST1
Maintenance Domain Name Format... character-string
Maintenance Domain Name Value.... MD-12L0
Level........................... 0
Associated CFM Services..... (Link Level ): MA-INST1-1
MIP Creation.................... None
------------------------------------------------------------------
Maintenance Domain Name..... MD-INST2
Maintenance Domain Name Format... character-string
Maintenance Domain Name Value.... MD-12L3
Level........................... 3
Associated CFM Services..... (Link Level ): MA-INST2-1
MIP Creation.................... None
------------------------------------------------------------------
```

Figure 9-4: Example output from **show ethernet cfm domain MD-INST1 details**

```
awplus#show ethernet cfm domain MD-INST1 details

Maintenance Domain Name..... MD-INST1
Maintenance Domain Name Format... character-string
Maintenance Domain Name Value.... MD-12L0
Level........................... 0
Associated CFM Services..... (Link Level ): MA-INST1-1
MIP Creation.................... None
------------------------------------------------------------------
```

Table 9-2: Parameters in the output from **show ethernet cfm domain details**

Parameter	Description
`Domain Name`	The Maintenance Domain name for the managed object.
`Domain Name Format and Value`	The Maintenance Domain Name Format and Value. The format is one of the following: character-string DNS MAC No name
`Level`	The level for the domain.
`Associated CFM Services`	The Maintenance Associations (MA) instance names.
`MIP Creation`	The MIP creation value.

Related commands ethernet cfm domain-name

service ma-name

show ethernet cfm details

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show ethernet cfm errorlog

Overview Use this command to list the CFM Errors that are in the CFM Errors Event List, starting from the oldest at the top to the latest at the end.

Syntax `show ethernet cfm errorlog domain <domain-name>`

Parameter	Description
<domain-name>	Specify the domain name value.

Mode Privileged Exec

Usage notes When a new error is detected for a Maintenance Association (MA) that is associated with a Maintenance Domain (MD), and such is due to an error from a received or missing CCM from a Remote MEP, an event is logged to the CFM Errors Event List.

Example To show the list of errors for an MD named “MD-INST2”, use the command:

```
awplus# show ethernet cfm errorlog domain MD-INST2
```

Output Figure 9-5: Example output from **show ethernet cfm errorlog domain MD-INST2**

```
awplus#show ethernet cfm errorlog domain MD-INST2

CFM Service Name  Level VLAN MEPID Remote MAC      Error Reason
------------------------------------------------------------------
MA-INST2-1        0     0    12    0000.0000.0000  Remote MEP Down
```

Table 9-3: Parameters in the output from **show ethernet cfm errorlog domain MD-INST2**

Parameter	Description
Level	The level configured for the MD.
VLAN	The VLAN ID used by the MA if any, otherwise is "0".
MEPID	The MEP ID of the local MEP that detected the error.
Remote MAC	The source MAC address of the received CCM causing the error if known, 0000.0000.0000 otherwise.

Table 9-3: Parameters in the output from **show ethernet cfm errorlog domain MD-INST2** (cont.)

Parameter	Description
`Error Reason`	One of the following: "Remote MEP Down" - an RMEPCCMDefect has been declared for this remote MEP. CCMs have not been received from this remote MEP within the CCM interval. "MEP Configuration" - the CCM received from the remote MEP has the same MEP ID as the local MEP that received the CCM. For unicast remote MEPs this error can also indicate that even though the CCM received from the remote MEP has an MEP ID that matches a configured remote MEP ID in the MA, the source MAC address differs from the configured MAC address for that remote MEP. "Forwarding Loop" - the CCM received from the remote MEP has an MEP ID that matches a configured local MEP ID in the MA, and also has the same source MAC address as the local MEP's MAC address that received the CCM. "Cross Connected" - a xconCCMdefect was detected.
`CFM Service Name`	The name of the MA associated with the MD for this error(s).

Related commands

clear ethernet cfm errorlog

ethernet cfm domain-name

ethernet cfm mep

mep crosscheck

service ma-name

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show ethernet cfm maintenance-points local mep

Overview Use this command to show one or more Local MEPs, and their configuration and status in summary format. Options include the ability to show Local MEP(s) for a given interface with further option to show statistics counters. Another option is to show Local MEPs for a given Maintenance Association (MA) and Maintenance Domain (MD) either for statistics counters, or for one specific Local MEP with either detailed information or statistics counters.

Syntax

```
show ethernet cfm maintenance-points local mep interface <port> [counters]
```

```
show ethernet cfm maintenance-points local mep domain <domain-name> service <ma-name> [counters]
```

```
show ethernet cfm maintenance-points local mep domain <domain-name> service <ma-name> mep <mep-id> {details|counters}
```

Parameter	Description
`interface`	Specify the interface for which Local MEP(s) are to be shown.
`<interface-name>`	Specify the interface by name.
`counters`	Specify that counter statistics are to be shown.
`domain`	Specify the Maintenance Domain that Local MEP(s) are to be shown for. Both this and service must be specified.
`<domain-name>`	Specify the Maintenance Domain's CLI instance name.
`service`	Specify the Maintenance Association that the Local MEP(s) are to be shown for. Both this and domain must be specified.
`<ma-name>`	Specify CLI name that identifies the service (Maintenance Association (MA)) instance of interest.
`mep`	Specify one particular Local MEP of interest.
`<mep-id>`	Specify the Local MEP instance by MEP-id.
`details`	Specify that details are to be included in the output.

Mode User Exec/Privileged Exec

Examples To show the configuration and status of all the Local MEP(s) on an interface, use the command:

```
awplus# show ethernet cfm maintenance-points local mep interface port1.0.2
```

To show details of a specific Local MEP on an MA and its associated MD, use the command:

```
awplus# show ethernet cfm maintenance-points local mep domain
MD-INST1 service MA-INST1-1 mep 12 details
```

Output Figure 9-6: Example output from **show ethernet cfm maintenance-points local mep interface port1.0.2**

```
awplus#show ethernet cfm maintenance-points local mep interface
port1.0.2

Service Name    MEPID     Dir     Interface     State     Defect
-----------------------------------------------------------------
MA-INST1-1      12        D       port1.0.2     En        ..3..
```

Table 9-4: Parameters in the output from **show ethernet cfm maintenance-points local mep interface <interface-name>**

Parameter	Description
Service Name	The MA service name.
MEPID	The MEP ID of the local MEP of interest within the MA.
Dir	The direction of this local MEP: D - Down MEP. U - Up MEP. Note: Only Down is currently supported.
Interface	The interface on which the local MEP resides.
State	Whether the local MEP's CCM processing is enabled “En” or disabled “Dis”.
Defect	Defect bit list <dbl> indicating which of 5 possible defects are currently being detected with each bit showing the detected <defect-number> or . if there is no defect.

Figure 9-7: Example output from **show ethernet cfm maintenance-points local mep domain MD-INST1 service MA-INST1-1 mep 12 details**

```
awplus#show ethernet cfm maintenance-points local mep domain
MD-INST1 service MA-INST1-1 mep 12 details

Domain Name..................... MD-INST1
MA Service Name................. MA-INST1-1
MA Primary VLAN................. 0
MEP ID.......................... 12
Direction....................... Down
Interface....................... port1.0.2
    MEP Active State............ True
    CC State.................... Enabled
    CC Type..................... Multicast
    PDU VLAN Priority........... 7
    MAC-address................. 000c.2526.95a1
    Tx-RDI...................... True
    Current Defects............. 3 (someRMEPCCMdefect)
    Current Highest Defect Alarm.. 4 (someRMEPCCMdefect)
    Alarm Minimum Defect........ 2 (someMACstatusDefect)
    Alarm Trip Time............. AUTO (2.5 seconds)
    Alarm Reset Time............ AUTO (10 seconds)
    Configured Remote MEPs...... 21
    Missing Remote MEPs......... 21
    Error CCM Reason............ N/A
    Last Error CCM.............. N/A
    Cross-connect Defect Reason... N/A
    Last Cross Connect CCM...... N/A
```

Table 9-5: Parameters in the output from **show ethernet cfm maintenance-points local mep domain <domain-name> service <ma-name> mep <mep-id> details**

Parameter	Description
`Domain Name and MA Service Name`	Uniquely identify the MD and MA this local MEP is associated with.
`MA Primary VLAN`	The VLAN used by this MEP. A link-local MEP VLAN is indicated by "-".
`MEP ID`	The local MEP's ID.
`Direction`	The direction of the local MEP, either Down or Up.
`Interface`	The Interface port or Interface lag that the local MEP is configured against.
`MEP Active State`	The MEP's configured administrative state: Up: True Down: False.

Table 9-5: Parameters in the output from **show ethernet cfm maintenance-points local mep domain <domain-name> service <ma-name> mep <mep-id> details** (cont.)

Parameter	Description
CC State	The MEP's CCM configured administrative state: Up: Enable Down: Disable.
CC Type	The configured CCM sending and receiving type, either multicast or unicast. If not yet configured, it shows as None.
Tx-RDI	Whether this local MEP is sending RDI or not. An RDI is sent when one or more of the following defects have been declared by the local MEP: someRMEPCCMdefect someMACstatusDefect errorCCMdefect xconCCMdefect
Current Defects	A list of defects the local MEP is currently detecting. It shows the defect(s), as both a defect priority and name.
Current Highest Defect Alarm	The highest defect priority that has been encountered while the local MEP has been in an alarm state.
Alarm Minimum Defect	The minimum defect the local MEP has to see before declaring an alarm.
Alarm Trip Time	The amount of time the defect has to exist before an alarm is declared.
Configured Remote MEP IDs	A comma separated list of configured remote MEPs (by MEP IDs) known by this local MEP. If the remote MEP also has a configured unicast MAC address, the MEP ID will also include -HHHH.HHHH.HHHH.
Missing Remote MEPs	The remote MEPs (by MEP ID) that have been configured against this local MEP but have not been heard from.

Table 9-5: Parameters in the output from **show ethernet cfm maintenance-points local mep domain <domain-name> service <ma-name> mep <mep-id> details** (cont.)

Parameter	Description
`Error CCM Reason`	The reason that the local MEP is detecting the errorCCMdefect condition (if any): Wrong MEP ID Received - CCM received with correct level and MAID, but MEP ID has not been configured in this MA. My MEP ID Received - CCM received with correct level and MAID, but an MEP ID that is the same as a local MEP in this MA. My MEP ID Received (loop) - as above, but the CCM received also has the same MAC address as the local MEP in the MA. CCM Interval Mismatch - CCM received with correct level and MAID, but CCM interval does not match that configured for this MA. MAC address mismatch - for a configured unicast RMEP (via crosscheck) the MAC address did not match the provisioned value in the associated MA. N/A - indicates there is no error CCM defect being detected.
`Last Error CCM`	If an errorCCMdefect condition is detected, portions of the CCM that caused this condition are displayed.
`Cross Connect Defect Reason`	The reason that the local MEP is detecting the xconCCMdefect condition (if any): Wrong MAID - CCM received with correct level but incorrect MAID (mismatch in the domain name and/or short MA name versus configured). Wrong Level - CCM received with a level that is lower than the level configured for this local MEP's domain. N/A - indicates there is no error CCM defect being detected.
`Last Cross Connect CCM`	If a xconCCMdefect condition is detected, portions of the CCM that caused this condition are displayed.

Related commands

clear mep counter

ethernet cfm mep

show ethernet cfm details

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show ethernet cfm maintenance-points remote mep

Overview Use this command to show one or more Ethernet CFM maintenance points, namely Remote Maintenance End Points (MEPs) within a given Maintenance Association (MA) and its associated Maintenance Domain (MD), and their configuration and status in summary format. Options include the ability to show an individual Remote MEP in detail.

Syntax

```
show ethernet cfm maintenance-points remote mep domain
<domain-name> service <ma-name> [{mac <rmep-mac-address>|rmep
<mep-id>} details]
```

Parameter	Description
`domain`	Specify the Maintenance Domain that Remote MEP(s) are to be shown for.
`<domain-name>`	Specify the Maintenance Domain's CLI instance name.
`service`	Specify the Maintenance Association that the Remote MEP(s) are to be shown for.
`<ma-name>`	Specify the service's (Maintenance Association (MA)) CLI instance name.
`mac`	Specify the remote MEP of interest by its MAC address.
`<rmep-mac-address>`	Specify the value of the remote MEP's MAC address using the format HHHH.HHHH.HHHH where H is a hexadecimal digit.
`rmep`	Specify the remote MEP of interest by its ID.
`<mep-id>`	Specify the value of the remote MEP's ID in the range 1 to 8191.

Mode User Exec/Privileged Exec

Example To show all the remote MEP(s)'s status for this MA and MD in summary form, use the command:

```
awplus# show ethernet cfm maintenance-points remote mep domain
MD-INST1 service MA-INST1-1
```

To show a specific remote MEP by its ID in detail, use the command:

```
awplus# show ethernet cfm maintenance-points remote mep domain
MD-INST1 service MA-INST1-1 rmep 21 details
```

To show a specific remote MEP by its MAC address in detail, use the command:

```
awplus# show ethernet cfm maintenance-points remote mep domain
MD-INST1 service MA-INST1-1 mac 000c.2526.95bf details
```

Output Figure 9-8: Example output from **show ethernet cfm maintenance-points remote mep domain MD-INST1 service MA-INST1-1**

```
awplus#show ethernet cfm maintenance-points remote mep domain
MD-INST1 service MA-INST1-1

CFM Domain Name: MD-INST1
CFM Service Name: MA-INST1-1
       RX    RX   Port  Intf
MEPID  CCM   RDI  Stat  Stat
----------------------------
21     Yes   No   Up    Up
```

Figure 9-9: Example output from **show ethernet cfm maintenance-points remote mep domain MD-INST1 service MA-INST1-1 rmep 21 details**

```
awplus#show ethernet cfm maintenance-points remote mep domain
MD-INST1 service MA-INST1-1 rmep 21 details

CFM Service Name..... MA-INST1-1
CFM Domain Name...... MD-INST1
Remote MEPID......... 21
Receiving CCMs....... Yes
Rx RDI............... No
MAC Address.......... 000c.2526.95bf
Port Status.......... Up
Interface Status..... Up
```

Figure 9-10: Example output from **show ethernet cfm maintenance-points remote mep domain MD-INST1 service MA-INST1-1 mac 000c.2526.95bf details**

```
awplus#show ethernet cfm maintenance-points remote mep domain
MD-INST1 service MA-INST1-1 mac 000c.2526.95bf details

CFM Service Name..... MA-INST1-1
CFM Domain Name...... MD-INST1
Remote MEPID......... 21
Receiving CCMs....... Yes
Rx RDI............... No
MAC Address.......... 000c.2526.95bf
Port Status.......... Up
Interface Status..... Up
```

Table 9-6: Parameters in the output from **show ethernet cfm maintenance-points remote mep**

Parameter	Description
`CFM Domain Name and CFM Service Name`	The instance identifiers that uniquely identify the MA and MD for the remote MEP(s) of interest.
`Remote MEPID`	The remote MEP ID that is configured for this MA.
`Receiving CCMs`	The current state of the 802.1ag remote MEP state machine: Yes - RMEP_OK. CCMs are being received without any error. Wait - RMEP_START. Still preparing to receive remote MEP CCMs without a timeout occurring. Failed - RMEP_FAILED. While waiting to receive CCMs from a remote MEP, a timeout occurred. - - the state machine is not running.
`RX RDI`	The current RDI being received from this remote MEP: True - the last CCM received from the remote MEP has the RDI set. This means the remote MEP itself is seeing one of the following defects: someRMEPCCMDefect, someMACstatusDefect, errorCCMdefect, xconCCMdefect. False - the last CCM received from the remote MEP does not have its RDI set.
`MAC Address`	The configured or discovered MAC address of the remote MEP.
`Port Status`	If the CCM was received with a port status TLV, this indicates the last value received, or "-" if none received.
`Interface Status`	If the CCM was received with an interface status TLV, this indicates the last value received, or "-" if none received.

Related commands

ethernet cfm domain-name

mep crosscheck

service ma-name

show ethernet cfm details

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show ethernet cfm service

Overview Use this command to show the Ethernet CFM Services (Maintenance Associations (MA)) configuration in summary format, or show a specified MA with detailed information.

Syntax

```
show ethernet cfm service [<ma-name> domain <domain-name>
details]
```

Parameter	Description
<ma-name>	The CLI name that identifies the service (Maintenance Association (MA)) instance of interest.
domain	Specify the domain name by name.
<domain-name>	The CLI name that identifies this Maintenance Domain instance.

Mode User Exec/Privileged Exec

Example To show details for all MAs in summary form, use the command:

```
awplus# show ethernet cfm service
```

To show a specified MA in detailed form, use the command:

```
awplus# show ethernet cfm service MA-INST2-1 domain MD-INST2
details
```

Output Figure 9-11: Example output from **show ethernet cfm service**

```
awplus#show ethernet cfm service

CFM Domain Name     CFM Service Name           VLAN       Defect
------------------------------------------------------------------
MD-INST1            MA-INST1-1                 NONE       .....
MD-INST2            MA-INST2-1                 NONE       ..3..
```

Table 9-7: Parameters in the output from **show ethernet cfm service**

Parameter	Description
CFM Domain Name	The Maintenance Domain name for the managed object.
CFM Service Name	The Maintenance Associations (MA) instance name.

Table 9-7: Parameters in the output from **show ethernet cfm service** (cont.)

Parameter	Description
VLAN	The Primary VLAN.
Defect	A list of defects detected by the MA's Local MEPs. The defects shown can be: 1 - someRDIdefect is declared 2 - someMACstatusDefect is declared 3 - someRMEPCCMdefect is declared 4 - errorCCMdefect is declared 5 - xconCCMdefect is declared

Figure 9-12: Example output from **show ethernet cfm service MA-INST2-1 domain MD-INST2 details**

```
awplus#show ethernet cfm service MA-INST2-1 domain MD-INST2
details

CFM Service Name.............. MA-INST2-1
CFM Domain Name............... MD-INST2
CFM Domain Level.............. 3
Primary VLAN.................. -

Maintenance Assoc Name Format... string
Maintenance Assoc Name Value.... MA-12V100
CCM Transmission Interval..... 1 second
Local MEPs.................... MEP DOWN
                               12 (interface port1.0.2)

Configured Remote MEPs........ 21
Missing Remote MEPs........... 21
Current MEP Defects........... 3 (someRMEPCCMdefect)
MIP Creation.................. None
```

Table 9-8: Parameters in the output from **show ethernet cfm service <ma-name> domain <domain-name> details**

Parameter	Description
CFM Service Name	The Maintenance Associations (MA) instance name.
CFM Domain Name	The Maintenance Domain name for the managed object.
CFM Domain Level	The level of the domain.
Primary VLAN	The Primary VLAN that was configured (if any).

Table 9-8: Parameters in the output from **show ethernet cfm service <ma-name> domain <domain-name> details** (cont.)

Parameter	Description
`Maintenance Assoc Name Format and Value`	The name and name format of the MA. The name format is one of the following: ICC - ICC string based name format Integer - Integer based name format Primary-vid - Primary VLAN based name format String - Character string based name format VPN-ID - VPN-ID based name format
`CCM Transmission Interval`	The CCI that was configured for this MA. It can be one of the following: 3 - CCI of 100 milliseconds 4 - CCI of 1 second (default) 5 - CCI of 10 seconds 6 - CCI of 1 minute 7 - CCI of 10 minutes
`Local MEPs`	A list of the Local MEPs configured for this MA. For each MEP, it displays the MEP direction Up or Down, its MEP-id, and the interface it was configured on.
`Configured Remote MEPs`	A list of Remote MEPs by MEP-id.
`Missing Remote MEPs`	A list of the configured Remote MEPs that this MA has not received any CCM messages from within 3.5 times the configured CCI.
`Defect`	A list of defects detected by the MA's Local MEPs. The defects shown can be: 1 - someRDIdefect is declared 2 - someMACstatusDefect is declared 3 - someRMEPCCMdefect is declared 4 - errorCCMdefect is declared 5 - xconCCMdefect is declared

Related commands

ethernet cfm domain-name

ethernet cfm mep

mep crosscheck

service ma-name

show ethernet cfm details

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show mep-alarm status

Overview Use this command to show any alarms that have been declared by Local MEPs, and the defect(s) that caused the alarm.

Syntax

```
show mep-alarm status
```

Mode User Exec/Privileged Exec

Usage notes A Local MEP is used to detect connectivity faults with other remote MEPs that are in the same Maintenance Association (MA) and Maintenance Domain (MD) as the Local MEP. A Local MEP looks first for connectivity defects, and if these defects persist for a long enough period of time (typically 2.5 seconds), then an alarm is declared.

Example To show the alarms on local MEPs, use the command:

```
awplus# show mep-alarm status
```

Output Figure 9-13: Example output from **show mep-alarm status**

```
awplus#show mep-alarm status

CFM Domain Name        CFM Service Name         MEP   Active Alarm
-----------------------------------------------------------------
MD-INST1               MA-INST1-1               12    someRMEPCCM
```

Table 9-9: Parameters in the output from **show mep-alarm status**

Parameter	Description
CFM Domain Name	The domain name.
CFM Service Name	The MA name.
Active Alarms	The highest priority defect causing the alarm, one of the following: someRDI, someMACstatus, someRMEPCCM, errorCCM, or xconCCM.
MEP	The local MEP's ID.

Related commands

ethernet cfm mep

mep (FNG attributes)

mep crosscheck

Command changes

Version 5.4.7-1.1: command added

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

10 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 385
- "clear log" on page 386
- "clear log buffered" on page 387
- "clear log external" on page 388
- "clear log permanent" on page 389
- "copy buffered-log" on page 390
- "copy permanent-log" on page 391
- "default log buffered" on page 392
- "default log console" on page 393
- "default log email" on page 394
- "default log external" on page 395
- "default log host" on page 396
- "default log monitor" on page 397
- "default log permanent" on page 398
- "log buffered" on page 399
- "log buffered (filter)" on page 400
- "log buffered exclude" on page 403
- "log buffered size" on page 406
- "log console" on page 407

- "log console (filter)" on page 408
- "log console exclude" on page 411
- "log email" on page 414
- "log email (filter)" on page 415
- "log email exclude" on page 418
- "log email time" on page 421
- "log external" on page 423
- "log external (filter)" on page 425
- "log external exclude" on page 428
- "log external rotate" on page 431
- "log external size" on page 433
- "log facility" on page 434
- "log host" on page 436
- "log host (filter)" on page 438
- "log host exclude" on page 441
- "log host source" on page 444
- "log host startup-delay" on page 445
- "log host time" on page 447
- "log monitor (filter)" on page 449
- "log monitor exclude" on page 452
- "log permanent" on page 455
- "log permanent (filter)" on page 456
- "log permanent exclude" on page 459
- "log permanent size" on page 462
- "log-rate-limit nsm" on page 463
- "log trustpoint" on page 464
- "show counter log" on page 465
- "show exception log" on page 466
- "show log" on page 467
- "show log config" on page 469
- "show log external" on page 471
- "show log permanent" on page 472
- "show running-config log" on page 473
- "unmount" on page 474

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 external

Overview Use this command to delete the external log file from the USB storage device it is stored on.

If the external log is rotating between multiple files, this command deletes all those files, not just the most recent one.

Syntax

```
clear log external
```

Mode Privileged Exec

Example To delete the external log file, use the command:

```
awplus# clear log external
```

Related commands

default log external

log external

log external (filter)

log external exclude

log external rotate

log external size

show log config

show log external

unmount

Command changes Version 5.4.7-1.1: command added

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 131 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
```

To copy the buffered log file onto a USB storage device and name the file "buffered-log.log", use the command:

```
awplus# copy buffered-log usb:/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 131 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
```

To copy the permanent log file onto a USB storage device and name the file "permanent-log.log", use the command:

```
awplus# copy permanent-log usb:/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 external

Overview Use this command to restore the default settings for the external log. By default, the size of the external log is 50 kB, it rotates through 1 additional file, and it accepts messages with a severity level of notices and above.

Note that this command does not clear the configured filename for the external log.

Syntax
```
default log external
```

Mode Global Configuration

Example To restore the default settings for the external log, use the commands:

```
awplus# configure terminal
awplus(config)# default log external
```

Related commands
clear log external
log external
log external (filter)
log external exclude
log external rotate
log external size
show log config
show log external
unmount

Command changes Version 5.4.7-1.1: command added

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

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

To add a filter to send all messages containing the text "Bridging initialization" to the buffered log, use the following commands:

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

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

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

To remove a filter that sends all messages containing the text "Bridging initialization" to the buffered log, use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered msgtext Bridging initialization
```

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

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

To remove a default filter that includes sending **critical**, **alert** and **emergency** level messages to the console, use the following commands:

```
awplus# configure terminal
awplus(config)# no log console level critical
```

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

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

To create a filter to send all messages containing the text “Bridging initialization”, to the email address admin@homebase.com, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@homebase.com msgtext "Bridging initialization"
```

To create a filter to send messages with a severity level of **informational** and above to the email address admin@alliedtelesis.com, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com level informational
```

To stop the device emailing log messages emailed to the email address admin@alliedtelesis.com, use the following commands:

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

To remove a filter that sends all messages generated by EPSR that have a severity of **notices** or higher to the email address admin@homebase.com, use the following commands:

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

To remove a filter that sends messages with a severity level of **informational** and above to the email address admin@alliedtelesis.com, use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@alliedtelesis.com level informational
```

Related commands

default log email

log email

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 external

Overview Use this command to enable external logging. External logging sends syslog messages to a file on a USB storage device.

If the file does not already exist on the storage device, it (and any specified subdirectory) will be automatically created. If the file already exists, messages are appended to it.

Use the **no** variant of this command to disable external logging.

Syntax

```
log external <filename>
no log external
```

Parameter	Description
<filename>	The file and optionally directory path to store the log messages in. See Introduction on page 131 for valid syntax.

Default External logging is disabled by default.

Mode Global Configuration

Usage notes We strongly recommend using ext3 or ext4 as the file system on the external storage device. These file systems have a lower risk of file corruption occurring if the switch or firewall loses power.

You should also unmount the storage device before removing it from the switch or firewall, to avoid corrupting the log file. To unmount the device, use the **unmount** command.

Example To save messages to a file called “messages.log” in a directory called “log” on a USB storage device, use the command:

```
awplus# configure terminal
awplus(config)# log external usb:/log/messages.log
```

Related commands

clear log external

default log external

log external (filter)

log external exclude

log external rotate

log external size

show log config

show log external

unmount

Command changes Version 5.4.7-1.1: command added

log external (filter)

Overview Use this command to create a filter to select messages to be sent to the external log. You can include messages 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 external log.

Syntax

```
log external [level <level>] [program <program-name>] [facility
<facility>] [msgtext <text-string>]
```

```
no log external [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Filter messages to the external log by severity level.	
<level>	The minimum severity of message to send to the external 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 external log by program. Include messages from a specified program in the external 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)

Parameter	Description	
	`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`	Filter messages to the external log by syslog facility.	
<facility>	Specify one of the following syslog facilities to include messages from in the 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

Parameter	Description
`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 external log has a filter to select messages whose severity level is "notices (5)" or higher. This filter may be removed using the **no** variant of this command.

Mode Global Configuration

Examples To add a filter to send all messages generated by EPSR that have a severity of **notices** or higher to the external log, use the following commands:

```
awplus# configure terminal
awplus(config)# log external level notices program epsr
```

To add a filter to send all messages containing the text "Bridging initialization" to the external log, use the following commands:

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

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

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

To remove a filter that sends all messages containing the text "Bridging initialization" to the external log, use the following commands:

```
awplus# configure terminal
awplus(config)# no log external msgtext Bridging initialization
```

Related commands

clear log external

default log external

log external

log external exclude

log external rotate

log external size

show log config

show log external

unmount

Command changes Version 5.4.7-1.1: command added

log external exclude

Overview Use this command to exclude specified log messages from the external 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 external exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log external 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 external exclude msgtext example of
irrelevant message
```

Related commands

clear log external

default log external

log external

log external (filter)

log external rotate

log external size

show log config

show log external

unmount

Command changes Version 5.4.7-1.1: command added

log external rotate

Overview Use this command to configure the number of files that the external log can rotate through.

Use the **no** variant of this command to return to the default.

Syntax

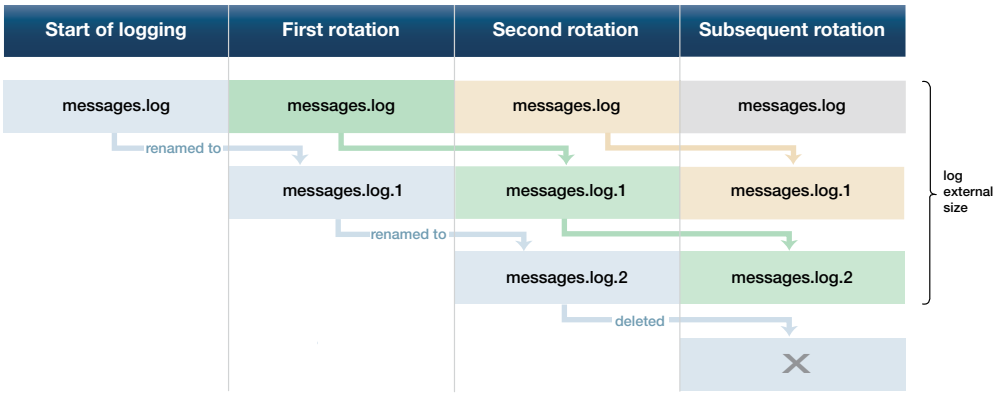
```
log external rotate <0-255>
no log external rotate
```

Parameter	Description
<0-255>	The number of additional files to rotate through. Note that the device rotates between the initial file and the number of additional files specified by this value - see the Usage section below.

Default The default is 1, which rotates between the initial file and 1 additional file (for example, rotates between messages.log and messages.log.1)

Mode Global Configuration

Usage notes The device rotates between the initial file and the number of additional files specified by this command. For example, the diagram below shows how setting rotate to 2 makes the device rotate through 3 files.



Note that if you set rotate to 0, and the external log file becomes full, then the device deletes the full log file and creates a new (empty) file of the same name to save messages into. For this reason, we recommend setting rotate to at least 1.

Example To set the rotation value to 2, and therefore rotate between 3 files, use the commands:

```
awplus# configure terminal
awplus(config)# log external rotate 2
```

Related commands clear log external

default log external

log external

log external (filter)

log external exclude

log external size

show log config

show log external

unmount

Command changes Version 5.4.7-1.1: command added

log external size

Overview Use this command to configure the total amount of size that the external log is permitted to use, in kilobytes. The maximum possible depends on the storage device's file system.

Note that if you are rotating between multiple files, this is the maximum size of all files, not of each individual file. For example, if you are rotating between 2 files (**log external rotate 1**), each file will have a maximum size of 25 kBytes by default.

Use the **no** variant of this command to return to the default size.

Syntax

```
log external size [<50-4194304>]
no log external size
```

Parameter	Description
<50-4194304>	The total amount of size that the external log is permitted to use, in kilobytes.

Default 50 kBytes

Mode Global Configuration

Example To configure a total log size of 100 kBytes, use the commands:

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

Related commands

clear log external

default log external

log external

log external (filter)

log external exclude

log external rotate

log external size

show log config

show log external

unmount

Command changes Version 5.4.7-1.1: command added

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 10-1: 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 10-1: 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

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 generated by EPSR that have a severity of **notices** or higher to a remote syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 level notices program epsr
```

To create a filter to send all messages containing the text “Bridging initialization”, to a remote syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 msgtext "Bridging
initialization"
```

To create a filter to send messages with a severity level of **informational** and above to the syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 level informational
```

To remove a filter that sends all messages generated by EPSR that have a severity of **notices** or higher to a remote syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.21 level notices program
epsr
```

To remove a filter that sends all messages containing the text “Bridging initialization”, to a remote syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.21 msgtext "Bridging
initialization"
```

To remove a filter that sends messages with a severity level of **informational** and above to the syslog server with IP address 10.32.16.21, use the following commands:

```
awplusawpluls# configure terminal
awplus(config)# no log host 10.32.16.21 level informational
```

Related commands

default log host

log host

log host exclude

log host source

log host time

show log config

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 exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log host 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 host 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

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 <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 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

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

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

To remove a default filter that includes sending everything to the terminal, use the following commands:

```
awplus# configure terminal
awplus(config)# no log monitor level debugging
```

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

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

To create a filter to send all messages containing the text "`Bridging initialization`", to the permanent log use the following commands:

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

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 10-1: 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 11: Parameters in output of the **show counter log** command

Parameter	Description
Total Received	Total number of messages received by the log
Total Received P0	Total number of Priority 0 (Emergency) messages received
Total Received P1	Total number of Priority 1 (Alert) messages received
Total Received P2	Total number of Priority 2 (Critical) messages received
Total Received P3	Total number of Priority 3 (Error) messages received
Total Received P4	Total number of Priority 4 (Warning) messages received
Total Received P5	Total number of Priority 5 (Notice) messages received
Total Received P6	Total number of Priority 6 (Info) messages received
Total Received P7	Total number of Priority 7 (Debug) messages received

Related commands show log config

show exception log

Overview This command displays the contents of the exception log.

Syntax

```
show exception log
```

Mode User Exec and Privileged Exec

Example To display the exception log, use the command:

```
awplus# show exception log
```

Output Figure 10-2: Example output from the **show exception log** command on a device

```
awplus#show exception log

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
2019 Sep 29 06:07:24 local7.debug awplus corehandler : Process imi (PID:775) signal
5, core dumped to /flash/imi-example-5.4.9-1.4-1-1569737243-775.tgz
------------------------------------------------------------------------
```

Output Figure 10-3: Example output from the **show exception log** command on a device that has never had an exception occur

```
awplus#show exception log
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
None
------------------------------------------------------------------------
awplus#
```

show log

Overview This command displays the contents of the buffered log.

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

Syntax

```
show log [tail [<10-250>]]
```

Parameter	Description
`tail`	Display only the latest log entries.
<10-250>	Specify the number of log entries to display.

Default By default the entire contents of the buffered log is displayed.

Mode User Exec, Privileged Exec and Global Configuration

Usage notes If the optional **tail** parameter is specified, only the latest 10 messages in the buffered log are displayed. A numerical value can be specified after the **tail** parameter to select how many of the latest messages should be displayed.

The **show log** command is only available to users at privilege level 7 and above. To set a user's privilege level, use the command:

```
awplus(config)# username <name> privilege <1-15>
```

Examples To display the contents of the buffered log use the command:

```
awplus# show log
```

To display the 10 latest entries in the buffered log use the command:

```
awplus# show log tail 10
```

Output Figure 10-4: Example output from **show log**

```
awplus#show log

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
2019 Sep 29 06:21:02 syslog.notice awplus syslog-ng[274]: syslog-ng starting up;
version='3.10.1'
2019 Sep 29 06:21:02 kern.notice awplus kernel: SCSI subsystem initialized
2019 Sep 29 06:21:03 kern.notice awplus kernel: gpio-addr-flash: probing 16-bit
flash bus
2019 Sep 29 06:21:03 kern.notice awplus kernel: number of CFI chips: 1
2019 Sep 29 06:21:03 kern.notice awplus kernel: 6 ofpart partitions found on MTD
device gpio-addr-flash
2019 Sep 29 06:21:03 kern.notice awplus kernel: Bridge firewalling registered
2019 Sep 29 06:21:04 kern.notice awplus kernel: Registering SWP/SWPB emulation
handler
2019 Sep 29 06:21:04 kern.notice awplus kernel: RAMDISK: squashfs filesystem found
at block 0
2019 Sep 29 06:21:04 kern.notice awplus kernel: random: real_init urandom read with
41 bits of entropy available
2019 Sep 29 06:21:04 kern.notice awplus kernel: scsi 0:0:0:0: Direct-Access    USB
FLASH DRIVE      8.07 PQ: 0 ANSI: 4
2019 Sep 29 06:21:04 kern.notice awplus kernel: random: nonblocking pool is
initialized
...
```

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 10-5: Example output from **show log config**

```
Facility: default

PKI trustpoints: example_trustpoint

Buffered log:
 Status ......... enabled
  Maximum size ... 100kb
  Filters:
 *1 Level ........ notices
    Program ...... any
    Facility ..... any
    Message text . any
  2 Level ........ informational
    Program ...... auth
    Facility ..... daemon
    Message text . any
  Statistics ..... 1327 messages received, 821 accepted by filter (2016 Oct 11
10:36:16)
Permanent log:
  Status ......... enabled
  Maximum size ... 60kb
  Filters:
  1 Level ........ error
    Program ...... any
    Facility ..... any
    Message text . any
 *2 Level ........ warnings
    Program ...... dhcp
    Facility ..... any
    Message text . "pool exhausted"
  Statistics ..... 1327 messages received, 12 accepted by filter (2016 Oct 11
10:36:16)
```

```
Host 10.32.16.21:
  Time offset .... +2:00
  Offset type .... UTC
  Source ......... -
  Secured ........ enabled
  Filters:
  1 Level ........ critical
    Program ...... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 1 accepted by filter (2016 Oct 11
10:36:16)
Email admin@alliedtelesis.com:
  Time offset .... +0:00
  Offset type .... Local
  Filters:
  1 Level ........ emergencies
    Program ...... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 0 accepted by filter (2016 Oct 11
10:36:16)
...
```

In the above example the '*' next to filter 1 in the buffered log configuration indicates that this is the default filter. The permanent log has had its default filter removed, so none of the filters are marked with '*'.

NOTE: *Terminal log and console log cannot be set at the same time. If console logging is enabled then the terminal logging is turned off.*

Related commands

show counter log

show log

show log permanent

show log external

Overview Use this command to display the contents of the external log, which is stored on a USB storage device.

Syntax

```
show log external [tail [<10-250>]]
```

Parameter	Description
`tail`	Display only the latest log entries.
<10-250>	Specify the number of log entries to display.

Mode Global Configuration

Privileged Exec

User Exec

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.

Example To display the last 5 entries in the external log, use the command:

```
awplus# show log external tail 5
```

Related commands

clear log external

default log external

log external

log external (filter)

log external exclude

log external rotate

log external size

show log config

unmount

Command changes Version 5.4.7-1.1: command added

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 10-6: Example output from **show log permanent**

```
awplus#show log permanent

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
2014 Jun 10 09:30:09 syslog.notice syslog-ng[67]: syslog-ng starting up;
version=\'2.0rc3\'
2014 Jun 10 09:30:09 auth.warning portmap[106]: user rpc not found, reverting to
user bin
2014 Jun 10 09:30:09 cron.notice crond[116]: crond 2.3.2 dillon, started, log
level 8
2014 Jun 10 09:30:14 daemon.err snmpd[181]: /flash/.configs/snmpd.conf: line 20:
Error: bad SUBTREE object
2014 Jun 10 09:30:14 user.info HSL[192]: HSL: INFO: Registering port port1.0.1
```

Related commands

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

unmount

Overview Use this command to unmount an external storage device. We recommend you unmount storage devices before removing them, to avoid file corruption. This is especially important if files may be automatically written to the storage device, such as external log files or AMF backup files.

Syntax

```
unmount usb
```

Parameter	Description
`usb`	Unmount the USB storage device.

Mode Privileged Exec

Example To unmount a USB storage device and safely remove it from the device, use the command:

```
awplus# unmount usb
```

Related commands

clear log external

log external

show file systems

show log config

show log external

Command changes Version 5.4.7-1.1: command added

11 Scripting Commands

Introduction

Overview This chapter provides commands used for command scripts.

Command List

- "activate" on page 476
- "echo" on page 477
- "wait" on page 478

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>	<1-65335> 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 port1.0.2 over a 10 second interval:

```
enable

show interface port1.0.2

wait 10

show interface port1.0.2
```

Related commands activate

echo

enable (Privileged Exec mode)

12 Interface Commands

Introduction

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

Command List

- "description (interface)" on page 480
- "interface (to configure)" on page 481
- "mru" on page 483
- "mtu" on page 484
- "service statistics interfaces counter" on page 485
- "show interface" on page 486
- "show interface brief" on page 489
- "show interface memory" on page 490
- "show interface status" on page 492
- "shutdown" on page 494

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

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: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • the loopback interface (lo) • a continuous range of interfaces separated by a hyphen (e.g. vlan10-20) • a comma-separated list (e.g. vlan1,vlan10-20). Do not mix interface types in a list. The specified interfaces must exist.

Usage notes A local loopback interface is one that is always available for higher layer protocols to use and advertise to the network. Although a local loopback interface is assigned an IP address, it does not have the usual requirement of connecting to a lower layer physical entity. This lack of physical attachment creates the perception of a local loopback interface always being accessible via the network.

Local loopback interfaces can be utilized by a number of protocols for various purposes. They can be used to improve access to the device and also increase its reliability, security, scalability and protection. In addition, local loopback interfaces can add flexibility and simplify management, information gathering and filtering.

One example of this increased reliability is for OSPF to advertise a local loopback interface as an interface-route into the network irrespective of the physical links that may be 'up' or 'down' at the time. This provides a higher probability that the routing traffic will be received and subsequently forwarded.

Mode Global Configuration

Examples The following example shows how to enter Interface mode to configure VLAN interface vlan1. Note how the prompt changes.

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

The following example shows how to enter Interface mode to configure the local loopback interface.

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)#
```

Related commands

ip address (IP Addressing and Protocol)

show interface

show interface brief

mru

Overview Use this command to set the Maximum Receive Unit (MRU) size for switch ports, where MRU is the maximum frame size (excluding headers) that switch ports can receive. For more information, see the Switching Feature Overview and Configuration Guide.

Use the **no** variant of this command to remove a previously specified Maximum Receive Unit (MRU) size for switch ports, and restore the default MRU size (1500 bytes) for switch ports.

NOTE: *The MRU sizes specify the payload only. For an IEEE 802.1q frame, provision is made (internally) for the following additional components:*

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

These additional components increase the frame size internally by 22 bytes. For example, the default frame size is 1522 bytes, including headers.

Syntax

```
mru <mru-size>
no mru
```

Parameter	Description
<mru-size>	68-16335. This value specifies the Maximum Receive Unit (MRU) size in bytes, where 1500 bytes is the default Ethernet MRU size for an interface.

Default The default MRU size is 1500 bytes for switch ports.

Mode Interface Configuration for switch ports.

Examples To configure an MRU of 16335 bytes on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# mru 16335
```

To restore the MRU default size of 1500 bytes on port1.0.2, use the commands:

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

Related commands show interface

mtu

Overview Use this command to set the Maximum Transmission Unit (MTU) size for 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
```

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.

Note that show interface output will only show MTU size for VLAN interfaces.

Examples To configure an MTU size of 1555 bytes on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# mtu 1555
```

To restore the MTU size to the default MTU size of 1500 bytes on vlan2, use the commands:

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

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.

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: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • the loopback interface (lo) • a continuous range of interfaces separated by a hyphen (e.g. vlan10-20) • a comma-separated list (e.g. vlan1,vlan10-20). Do not mix interface types in a list. The specified interfaces must exist.

Mode User Exec and Privileged Exec

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

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

```
awplus# show interface
```

Figure 12-1: Example output from the **show interface** command:

```
awplus#show interface
Interface port1.0.1
  Link is UP, administrative state is UP
  Hardware is Ethernet, address is 0000.cd38.026c
  index 5001 metric 1 mru 1500
  current duplex full, current speed 1000, current polarity mdix
  configured duplex auto, configured speed auto, configured polarity auto
  <UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
    input packets 2927667, bytes 224929311, dropped 0, multicast packets 1242629
    output packets 378084, bytes 54372424, multicast packets 1, broadcast packets 10
    input average rate : 30 seconds 5.19 Kbps, 5 minutes 8.16 Kbps
    output average rate: 30 seconds 6.04 Kbps, 5 minutes 73.89 Kbps
    input peak rate 268.60 Kbps at 2018/04/10 17:46:43
    output peak rate 6.81 Mbps at 2018/04/10 18:15:44
  Time since last state change: 7 days 01:58:10
...
```

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

```
awplus# show interface lo
```

Figure 12-2: 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
```

To display configuration and status information for interface vlan1, use the command:

```
awplus# show interface vlan1
```

Figure 12-3: Example output from the **show interface vlan1** command:

```
awplus#show interface vlan1
Interface vlan1
  Link is UP, administrative state is UP
  Hardware is VLAN, address is 0000.cd38.026c
  IPv4 address 192.168.1.1/24 broadcast 192.168.1.255
  index 301 metric 1 mtu 1500
  arp ageing timeout 300
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  SNMP link-status traps: Disabled
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 9, bytes 612, 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
    output peak rate 140 bps at 2018/04/10 16:40:56
  Time since last state change: 8 days 19:09:19
```

Related commands

ecofriendly lpi

mru

mtu

show interface brief

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

Output Figure 12-4: Example output from **show interface brief**

```
awplus#show interface brief
Interface              Status          Protocol
port1.0.1              admin up        down
port1.0.2              admin up        down
port1.0.3              admin up        down
port1.0.4              admin up        down
port1.0.5              admin up        down
port1.0.6              admin up        running
lo                     admin up        running
vlan1                  admin up        down
vlan2                  admin up        down
```

Table 12-1: 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 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: • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • 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.

Mode User Exec and Privileged Exec

Example To display the shared memory used by all interfaces, use the command:

```
awplus# show interface memory
```

To display the shared memory used by port1.0.1 and port1.0.3 to port1.0.4, use the command:

```
awplus# show interface port1.0.1,port1.0.3-port1.0.4 memory
```

Output Figure 12-5: Example output from the **show interface memory** command

```
awplus#show interface memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
port1.0.1    491535       512            1
port1.0.2    393228       512            1
port1.0.3    557073       512            1
...
lo           425997       512            1
po1          1179684      512            1
po2          1212453      512            1
sa3          1245222      512            1
```

Figure 12-6: Example output from **show interface <port-list> memory** for a list of interfaces

```
awplus#show interface port1.0.1,port1.0.3-port1.0.4 memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
port1.0.1    589842       512            1
port1.0.3    688149       512            1
port1.0.4    327690       512            1
```

Related commands

show interface brief

show interface status

show interface switchport

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: • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • 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.

Examples To display the status of port1.0.1 to port1.0.3, use the command:

```
awplus# show interface port1.0.1-port1.0.3 status
```

Table 13: Example output from the **show interface <port-list> status** command

```
awplus#show interface port1.0.1-port1.0.3 status
Port       Name               Status            Vlan Duplex   Speed Type
port1.0.1                     notconnect           1 auto      auto 1000BASE-T
port1.0.2                     notconnect           1 auto      auto 1000BASE-T
port1.0.3                     notconnect           1 auto      auto 1000BASE-T
```

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

```
awplus# show interface status
```

Table 14: Example output from the **show interface status** command

```
awplus#show interface status
Port      Name               Status             Vlan Duplex   Speed Type
port1.0.1 Trunk_Net          connected         trunk a-full  a-1000 1000BaseTX
port1.0.2 Access_Net1        connected             1 full      1000 1000BaseTX
port1.0.3 Access_Net1        disabled              1 auto      auto 1000BaseTX
...
```

Table 15: 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 VLAN mode is trunk, it displays **trunk** (it does not display the VLAN IDs). • When the VLAN mode is access, it displays the VLAN ID. • When the VLAN mode is private promiscuous, it displays the primary VLAN ID if it has one, and **promiscuous** if it does not have a VLAN ID. • When the VLAN mode is private host, it displays the primary and secondary VLAN IDs. • When the VLAN is dynamically assigned, it displays the current dynamically assigned VLAN ID (not the access VLAN ID), or **dynamic** if it has multiple VLANs dynamically assigned.
`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. For SFP bays, it displays **Unknown** if it does not recognize the type of SFP installed, or **Not present** if an SFP is not installed or is faulty.

Related commands

show interface

show interface memory

shutdown

Overview This command shuts down the selected interface. This administratively disables the link and takes the link down at the physical (electrical) layer.

Use the **no** variant of this command to disable this function and bring the link back up again.

Syntax

```
shutdown
no shutdown
```

Mode Interface Configuration

Usage notes If you shutdown an aggregator, the device shows the admin status of the aggregator and its component ports as “admin down”. While the aggregator is down, the device accepts **shutdown** and **no shutdown** commands on component ports, but these have no effect on port status. Ports will not come up again while the aggregator is down.

Example To shut down port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# shutdown
```

To bring up port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no shutdown
```

To shut down vlan2, use the commands:

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

To bring up vlan2, use the commands:

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

13 Port Mirroring and Remote Mirroring Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Port Mirroring and Remote Mirroring (also known as RSPAN).

For more information, see the Mirroring Feature Overview and Configuration Guide.

Command List

- "mirror interface" on page 496
- "remote-mirror interface" on page 498
- "show mirror" on page 500
- "show mirror interface" on page 501
- "show remote-mirror" on page 502
- "switchport remote-mirror-egress" on page 504
- "vlan mode remote-mirror-vlan" on page 505

mirror interface

Overview Use this command to define a mirror port and mirrored (monitored) ports and direction of traffic to be mirrored. The port for which you enter interface mode will be the mirror port.

The destination port is removed from all VLANs, and no longer participates in other switching.

Use the **no** variant of this command to disable port mirroring by the destination port on the specified source port.

Use the **none** variant of this command when using copy-to-mirror ACL and QoS commands.

Syntax

```
mirror interface <source-port-list> direction
{both|receive|transmit}
mirror interface none
no mirror interface <source-port-list>
no mirror interface none
```

Parameter	Description
<source-port-list>	The source switch ports to mirror. A port-list can be: • a port (e.g. port1.0.2) • a continuous range of ports separated by a hyphen, e.g. port1.0.1-port1.0.3 • a comma-separated list of ports and port ranges, e.g. port1.0.1,port1.0.2-port1.0.4 The source port list cannot include dynamic or static channel groups (link aggregators).
`direction`	Specifies whether to mirror traffic that the source port receives, transmits, or both.
`both`	Mirroring traffic both received and transmitted by the source port.
`receive`	Mirroring traffic received by the source port.
`transmit`	Mirroring traffic transmitted by the source port.
`none`	Specify this parameter for use with the **copy-to-mirror** parameter of: - the ACL (Access Control List) **access-list** and **ipv6 access-list** commands or - the QoS (Quality of Service) **default action** command. The **none** parameter lets you specify the destination port (the analyzer port) for the traffic without specifying a source mirror port.

Mode Interface Configuration

Usage notes

Use this command to send traffic to another device connected to the mirror port for monitoring.

For more information, see the Mirroring Feature Overview and Configuration Guide.

A mirror port cannot be associated with a VLAN. If a switch port is configured to be a mirror port, it is automatically removed from any VLAN it was associated with.

This command can only be applied to a single mirror (destination) port, not to a range of ports, nor to a static or dynamic channel group. Do not apply multiple interfaces with an interface command before issuing the mirror interface command. One interface may have multiple mirror interfaces.

Access control lists can be used to mirror a subset of traffic from the mirrored port by using the copy-to-mirror parameter in hardware ACL commands.

Example

To mirror traffic received and transmitted on port1.0.1 to destination port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# mirror interface port1.0.1 direction both
```

To enable use with the access-list (numbered hardware ACL for IP packets) ACL and default-action QoS commands to destination port1.0.1 without specifying a source port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# mirror interface none
```

To mirror all received or transmitted TCP traffic to analyzer port1.0.1, use the sample configuration snippet below:

```
awplus#show running-config

mls qos enable
access-list 3000 copy-to-mirror tcp any any
access-group 3000
!
interface port1.0.1
 mirror interface none
```

Related commands

access-list (numbered hardware ACL for IP packets)

access-list (numbered hardware ACL for MAC addresses)

default-action

ipv6 access-list (named IPv6 hardware ACL)

remote-mirror interface

Overview Use this command on the source device to specify the source port whose traffic is to be remote-mirrored (monitored), and the remote mirroring VLAN ID these mirrored frames will be tagged with when they egress from the source device. The port for which Interface Configuration mode is entered is the port via which the mirrored traffic egresses the source device towards the remote destination device.

Use the **no** variant of this command to disable remote mirroring of the specified mirrored port by the egress (destination) port on the source device.

Syntax

```
remote-mirror interface <port-list> direction
{both|receive|transmit} vlan <2-4090> [priority <0-7>]
```

```
remote-mirror interface none vlan <2-4090> [priority <0-7>]
```

```
no remote-mirror interface <port-list> [direction
{receive|transmit}]
```

```
no remote-mirror interface none
```

Parameter	Description
<port-list>	The ports from which to mirror traffic. A port-list can be: • a port (e.g. port1.0.1) • a continuous range of ports separated by a hyphen, e.g. port1.0.1-port1.0.4 • a comma-separated list of ports and port ranges, e.g. port1.0.1,port1.0.3-port1.0.4
`direction`	Specifies whether to mirror traffic that the source port receives, transmits, or both.
`both`	Mirroring traffic both received and transmitted by the source port.
`receive`	Mirroring traffic received by the source port.
`transmit`	Mirroring traffic transmitted by the source port.
`2-4090`	The VLAN ID of the remote mirroring VLAN that this mirrored traffic is to be tagged with at the egress port on the source device.
`priority`	The 802.1p priority tag to apply to mirrored packets.

Default No ports are set to be remote mirrored by default.

Mode Interface Configuration

Usage notes To prevent unwanted processing of mirrored traffic, we recommend configuring remote monitoring on the receiving device before configuring it on the source device.

This command can only be used to configure a single egress port on the source device, not a range of egress ports. Do not use the **interface** command with multiple interfaces before using this **remote-mirror interface** command. One egress (destination) port on the source device can transmit mirrored frames from up to four remote mirrored (source) ports.

The egress port on the source device can be associated with other VLANs in addition to the remote mirror VLAN, so it can function as an uplink for traffic from multiple VLANs. This command does not change the VLAN associations of the mirrored ports.

Only one port on the device can be configured as either a mirror port for port mirroring (**mirror interface** command) or as an egress port on the source device for remote mirroring (**remote-mirror interface** command).

All mirrored ports on a single device must use the same remote mirror VLAN and priority.

Access control lists can be used to mirror a subset of traffic from the mirrored port by using the copy-to-mirror parameter in hardware ACL commands.

Example To configure the source device to send all the traffic that it receives on remote-mirrored port port1.0.2 out egress port port1.0.1 tagged with remote mirroring VLAN ID 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# remote-mirror interface port1.0.2 direction
receive vlan 2
```

To stop port1.0.1 remote-mirroring traffic received on mirrored port port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no remote-mirror interface port1.0.2
direction receive
```

Related commands

access-list (numbered hardware ACL for IP packets)

access-list (numbered hardware ACL for MAC addresses)

default-action

mirror interface

remote-mirror interface

show remote-mirror

switchport remote-mirror-egress

vlan mode remote-mirror-vlan

show mirror

Overview Use this command to display the status of all mirrored ports.

Syntax

```
show mirror
```

Mode User Exec and Privileged Exec

Example To display the status of all mirrored ports, use the following command:

```
awplus# show mirror
```

Output Figure 13-1: Example output from the **show mirror** command

```
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.2
```

show mirror interface

Overview Use this command to display port mirroring configuration for a mirrored (monitored) switch port.

Syntax

```
show mirror interface <port>
```

Parameter	Description
<port>	The monitored switch port to display information about.

Mode User Exec, Privileged Exec and Interface Configuration

Example To display port mirroring configuration for port1.0.2, use the following commands:

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

Output Figure 13-2: Example output from the **show mirror interface** command

```
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.2
```

show remote-mirror

Overview Use this command to display information for remote-mirroring.

Syntax

```
show remote-mirror
```

Mode User Exec

Example To display information about remote mirroring, use the command:

```
awplus# show remote-mirror
```

Output Figure 13-3: Example output from **show remote-mirror**

```
awplus#show remote-mirror
Remote mirror information:
Remote mirror destination:
 Port: port1.0.3
 VLAN: 259
 User priority: 0

Monitored ports:
 port1.0.1
 direction: both

Remote mirror egress ports:

Remote mirror VLANs:
 VLAN 259
```

Table 13-1: Parameters in the output from **show remote-mirror**

Parameter	Description
`Remote mirror destination`	On the source device, this displays information about: • the egress port for the mirrored traffic on the source device • the remote mirroring VLAN ID this traffic is tagged with on egress • the user priority this traffic is tagged with on egress
`Monitored ports`	On the source device, this displays: • the ports being mirrored (monitored) • the direction—whether both received traffic, transmitted traffic or both are mirrored • 'none (via ACL)' if it is configured with the command **remote-mirror interface none** to allow ACLs to select the traffic to be mirrored

Table 13-1: Parameters in the output from **show remote-mirror** (cont.)

Parameter	Description
`Remote mirror egress ports`	On the destination device, this displays : • the remote mirror egress ports • the remote mirror VLANs they are associated with
`Remote mirror VLANs`	On source, destination and intermediate devices, this displays a list of any VLANs configured in remote mirror VLAN mode. To see a list of the ports associated with these VLANs, use the command **show vlan brief**.

Related commands

remote-mirror interface

switchport remote-mirror-egress

vlan mode remote-mirror-vlan

switchport remote-mirror-egress

Overview Use this command on the device receiving remote mirrored traffic to set the remote mirroring egress port for the specified remote mirroring VLAN. This port removes the remote mirror VLAN tagging before transmitting the mirrored traffic. Ingress traffic on this port is disabled.

Use the **no** variant of this command to reset the port to no longer function as a remote mirror egress port.

Syntax

```
switchport remote-mirror-egress vlan <vlan-id>
no switchport remote-mirror-egress
```

Parameter	Description
<vlan-id>	The port will transmit the mirrored traffic it receives from this remote mirror VLAN.

Default There is no remote mirror egress port by default.

Mode Interface Configuration for a switch port

Usage notes To prevent unwanted processing of mirrored traffic, we recommend configuring remote monitoring on the receiving device before configuring it on the source device.

This command would typically be used for the port that transmits the remote-mirrored traffic to a device that will analyze it. The port effectively functions as an access port in the remote mirror VLAN, with the added feature of not allowing ingress traffic on the port.

Example To set port1.0.2 on the destination device as the remote mirror egress port for mirrored traffic that is tagged with VLAN ID 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport remote-mirror-egress vlan 2
```

To unset port1.0.2 as a remote mirror egress port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport remote-mirror-egress
```

Related commands

remote-mirror interface

show remote-mirror

vlan mode remote-mirror-vlan

vlan mode remote-mirror-vlan

Overview Use this command to create a single VLAN or a range of VLANs in remote mirror mode to be used for remote mirroring.

Use the **no** variant of this command to remove the remote mirror VLAN from the VLAN database and its configurations.

Syntax

```
vlan [<vid>|<vid-range>] mode remote-mirror-vlan
no vlan [<vid>|<vid-range>]
```

Parameter	Description
<vid>	The VLAN ID of the remote mirroring VLAN to be created.
<vid-range>	The range of VLAN IDs for the remote mirroring VLANs to be created.

Default There is no remote mirror VLAN by default.

Mode VLAN Configuration

Usage notes This remote mirror VLAN needs to be configured on the remote mirroring source device, the destination (receiving) device, and any devices in between that are to forward the mirrored traffic. We recommend configuring this on the receiving device and intermediate devices before configuring the source device.

The remote mirror VLAN operates in a special mode— all traffic on the remote mirror VLAN is flooded, and no learning or CPU processing is done for packets in the VLAN. BPDU packets (link-local packets used to control features like spanning tree or AMF) are dropped on remote mirror VLANs.

Disabling the remote-mirroring VLAN on the source switch does not prevent the mirrored packets from being sent with the remote-mirror VLAN tag. To stop the mirroring, the command **no remote-mirror interface** must be used.

Example To create a VLAN with VLAN ID 3 in remote mirror VLAN mode, use the commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 3 mode remote-mirror-vlan
```

To remove the remote mirror VLAN with ID 3, use the commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 3
```

Related commands remote-mirror interface

show remote-mirror

switchport remote-mirror-egress

14 Alarm Monitoring Commands

Introduction

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

Command List

- "alarm facility epsr led" on page 509
- "alarm facility epsr relay" on page 510
- "alarm facility g8032 led" on page 511
- "alarm facility g8032 relay" on page 512
- "alarm facility input-alarm alarm-position" on page 513
- "alarm facility input-alarm led" on page 514
- "alarm facility input-alarm relay" on page 516
- "alarm facility link-down led" on page 518
- "alarm facility link-down relay" on page 519
- "alarm facility loopprot led" on page 520
- "alarm facility loopprot relay" on page 521
- "alarm facility main-pse led" on page 522
- "alarm facility main-pse relay" on page 523
- "alarm facility power-supply led" on page 524
- "alarm facility power-supply relay" on page 525
- "alarm facility pse-port led" on page 526
- "alarm facility pse-port relay" on page 527
- "alarm facility temperature led" on page 529
- "alarm facility temperature relay" on page 530

- "alarm facility ufo led" on page 531
- "alarm facility ufo relay" on page 532
- "debug alarm" on page 533
- "show alarm facility settings" on page 534
- "show alarm facility status" on page 535
- "show debugging alarm" on page 536

alarm facility epsr led

Overview Use this command to make the fault LED flash if EPSR detects that a link has gone down.

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility epsr led
no alarm facility epsr led
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use a relay to trigger an external alarm output, such as a buzzer, by using the command alarm facility epsr relay.

Example To flash the LED if EPSR detects that a link has gone down, use the commands:

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

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility epsr led
```

Related commands

alarm facility epsr relay

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches

alarm facility epsr relay

Overview Use this command to trigger an alarm relay if EPSR detects that a link has gone down.

This will activate the device that you have connected to the switch's relay output (for example, you could connect a buzzer to the relay output).

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility epsr relay
no alarm facility epsr relay
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use an alarm to flash the fault LED, by using the command alarm facility epsr led.

Example To trigger the alarm relay if EPSR indicates that a link has gone down, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility epsr relay
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility epsr relay
```

Related commands show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches

alarm facility g8032 led

Overview Use this command to make the fault LED flash if one or more G.8032 ERP instances are in the PROTECTION state.

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility g8032 led
no alarm facility g8032 led
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use a relay to trigger an external alarm output, such as a buzzer, by using the command alarm facility g8032 relay.

Example To flash the LED if one or more G.8032 ERP instances are in the PROTECTION state, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility g8032 led
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility g8032 led
```

Related commands alarm facility g8032 relay

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches

alarm facility g8032 relay

Overview Use this command to trigger an alarm relay if one or more G.8032 ERP instances are in the PROTECTION state.

This will activate the device that you have connected to the switch's relay output (for example, you could connect a buzzer to the relay output).

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility g8032 relay
no alarm facility g8032 relay
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use an alarm to flash the fault LED, by using the command alarm facility g8032 led.

Example To trigger the alarm relay if one or more G.8032 ERP instances are in the PROTECTION state, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility g8032 relay
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility g8032 relay
```

Related commands

alarm facility g8032 led

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches

alarm facility input-alarm alarm-position

Overview Use this command to specify whether an alarm occurs when the input contact opens or closes.

Then use the commands alarm facility input-alarm led and alarm facility input-alarm relay to specify whether the alarm triggers an LED or a relay.

Syntax

```
alarm facility input-alarm 1 alarm-position {open|close}
```

Parameter	Description
`input-alarm 1`	The input contact number. These switches have one input contact, so this must be 1.
`open`	An alarm will be triggered when the input contact opens
`close`	An alarm will be triggered when the input contact closes

Default Open

Mode Global Configuration

Example To trigger the alarm relay when the input contact closes, use the commands:

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

To return to the default state of **open**, use the commands:

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

Related commands

alarm facility input-alarm led

alarm facility input-alarm relay

show alarm facility settings

Command changes Version 5.4.9-1.1: **input-member** parameter added on IE510-28GSX switches

alarm facility input-alarm led

Overview Use this command to trigger an alarm if the input contact opens (or if it closes, if you have used the command alarm facility input-alarm alarm-position to specify closed).

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility input-alarm 1 led
no alarm facility input-alarm 1 led
```

Parameter	Description
input-alarm 1	The input contact number. These switches have one input contact, so this must be 1.

Default By default, there are no alarms

Mode Global Configuration

Usage notes By default, the input alarm will trigger if the input contact opens. You can change this to closed by using the command alarm facility input-alarm alarm-position.

You can also use a relay to trigger an external alarm output, such as a buzzer, by using the command alarm facility input-alarm relay.

Example To make the fault LED flash if the input contact opens, use the commands:

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

To make the fault LED flash if the input contact closes, use the commands:

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

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility input-alarm 1 led
```

Related commands

alarm facility input-alarm alarm-position

alarm facility input-alarm relay

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **input-member** and **output-member** parameters added on IE510-28GSX switches

alarm facility input-alarm relay

Overview Use this command to trigger an alarm relay if the input contact opens (or if it closes, if you have used the command alarm facility input-alarm alarm-position to specify closed).

This will activate the device that you have connected to the switch's relay output (for example, you could connect a buzzer to the relay output).

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility input-alarm 1 relay
no alarm facility input-alarm 1 relay
```

Parameter	Description
`input-alarm 1`	The input contact number. These switches have one input contact, so this must be 1.

Default By default, there are no alarms

Mode Global Configuration

Usage notes By default, the input alarm will trigger if the input contact opens. You can change this to closed by using the command alarm facility input-alarm alarm-position.

You can also use an alarm to flash the fault LED, by using the command alarm facility input-alarm led.

Examples To trigger the alarm relay if the input contact opens, use the commands:

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

To trigger the alarm relay if the input contact closes, use the commands:

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

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility input-alarm 1 relay
```

Related commands

alarm facility input-alarm alarm-position

alarm facility input-alarm led

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **input-member** and **output-member** parameters added on IE510-28GSX switches

alarm facility link-down led

Overview Use this command to make the fault LED flash if a link goes down on a particular switch port or ports.

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility link-down <port-list> led
no alarm facility link-down <port-list> led
```

Parameter	Description
<port-list>	The port or ports to monitor with this alarm. The port 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).

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use a relay to trigger an external alarm output, such as a buzzer, by using the command alarm facility link-down relay.

Example To flash the LED if port1.0.2 goes down, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility link-down port1.0.2 led
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility link-down port1.0.2 led
```

Related commands

alarm facility link-down relay

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches. Also, SNMP traps no longer required.

alarm facility link-down relay

Overview Use this command to trigger an alarm relay if a link goes down on a particular switch port or ports.

This will activate the device that you have connected to the switch's relay output (for example, you could connect a buzzer to the relay output).

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility link-down <port-list> relay
no alarm facility link-down <port-list> relay
```

Parameter	Description
<port-list>	The port or ports to monitor with this alarm. The port 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).

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use an alarm to flash the fault LED, by using the command alarm facility link-down led.

Example To trigger the alarm relay if port1.0.2 goes down, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility link-down port1.0.2 relay
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility link-down port1.0.2 relay
```

Related commands

alarm facility link-down led

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches. Also, SNMP traps no longer required.

alarm facility loopprot led

Overview Use this command to make the fault LED flash if the loop protection feature detects a loop.

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility loopprot led
no alarm facility loopprot led
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use a relay to trigger an external alarm output, such as a buzzer, by using the command alarm facility loopprot relay.

Example To flash the LED if loop protection detects a loop, use the commands:

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

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility loopprot led
```

Related commands

alarm facility loopprot relay

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches

alarm facility loopprot relay

Overview Use this command to trigger an alarm relay if the loop protection feature detects a loop.

This will activate the device that you have connected to the switch's relay output (for example, you could connect a buzzer to the relay output).

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility loopprot relay
no alarm facility loopprot relay
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use an alarm to flash the fault LED, by using the command alarm facility loopprot led.

Example To trigger the alarm relay if loop protection detects a loop, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility loopprot relay
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility loopprot relay
```

Related commands

alarm facility loopprot led

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches

alarm facility main-pse led

Overview Use this command to make the fault LED flash if the total power consumed by all of the PoE devices plugged into the switch exceeds the maximum PoE output permitted.

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility main-pse led
no alarm facility main-pse led
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use a relay to trigger an external alarm output, such as a buzzer, by using the command alarm facility main-pse relay.

Example To flash the LED if the total power consumed by all of the PoE devices plugged into the switch exceeds the maximum PoE output permitted, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility main-pse led
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility main-pse led
```

Related commands

alarm facility main-pse relay

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **input-member** and **output-member** parameters added on IE510-28GSX switches

alarm facility main-pse relay

Overview Use this command to trigger an alarm relay if the total power consumed by all of the PoE devices plugged into the switch exceeds the maximum PoE output permitted.

This will activate the device that you have connected to the switch's relay output (for example, you could connect a buzzer to the relay output).

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility main-pse relay
no alarm facility main-pse relay
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use an alarm to flash the fault LED, by using the command alarm facility main-pse led.

Example To trigger the alarm relay if the total power consumed by all of the PoE devices plugged into the switch exceeds the maximum PoE output permitted, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility main-pse relay
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility main-pse relay
```

Related commands

alarm facility main-pse led

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **input-member** and **output-member** parameters added on IE510-28GSX switches

alarm facility power-supply led

Overview Use this command to make the fault LED flash if a specified power supply is not supplying power.

Note that if both of the switch's power supplies stop supplying power, the switch's LED will not flash, because the switch will turn off. To trigger alarms if both power supplies go down, use the alarm relay instead (alarm facility power-supply relay).

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility power-supply <power-supply-number> led
no alarm facility power-supply led
```

Parameter	Description
`power-supply <power-supply-number>`	The number of the power supply you want to monitor with this alarm. The switch has two power supplies, so the number is 1 or 2.

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use a relay to trigger an external alarm output, such as a buzzer, by using the command alarm facility power-supply relay.

Example To flash the LED if power supply 2 goes down, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility power-supply 2 led
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility power-supply 2 led
```

Related commands

alarm facility power-supply relay

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **input-member** and **output-member** parameters added on IE510-28GSX switches

alarm facility power-supply relay

Overview Use this command to trigger an alarm relay if a specified power supply is not supplying power.

This will activate the device that you have connected to the switch's relay output (for example, you could connect a buzzer to the relay output).

Note that if both of the switch's power supplies stop supplying power, the switch will turn off and the relay will open, so the alarm will trigger.

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility power-supply <power-supply-number> relay
no alarm facility power-supply <power-supply-number> relay
```

Parameter	Description
`power-supply <power-supply-number>`	The number of the power supply you want to monitor with this alarm. The switch has two power supplies, so the number is 1 or 2.

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use an alarm to flash the fault LED, by using the command alarm facility power-supply led.

Example To trigger the alarm relay if power supply 2 goes down, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility power-supply 2 relay
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility power-supply 2 relay
```

Related commands

alarm facility power-supply led

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **input-member** and **output-member** parameters added on IE510-28GSX switches

alarm facility pse-port led

Overview Use this command to make the fault LED flash if a PoE device plugged into a port is consuming more than the maximum power output permitted for that port.

This alarm only triggers if the port exceeds the maximum power output permitted for that port. It does not trigger if you have configured a lower power budget for that port and the port exceeds your configured budget.

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility pse-port <port-list> led
no alarm facility pse-port <port-list> led
```

Parameter	Description
<port-list>	The port or ports to monitor with this alarm. The port 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).

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use a relay to trigger an external alarm output, such as a buzzer, by using the command alarm facility pse-port relay.

Example To flash the LED if a PoE device plugged into port1.0.2 is consuming more than the maximum power output permitted for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility pse-port port1.0.2 led
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility pse-port port1.0.2 led
```

Related commands

alarm facility pse-port relay

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches

alarm facility pse-port relay

Overview Use this command to trigger an alarm relay if a PoE device plugged into a port is consuming more than the maximum power output permitted for that port.

This will activate the device that you have connected to the switch's relay output (for example, you could connect a buzzer to the relay output).

This alarm only triggers if the port exceeds the maximum power output permitted for that port. It does not trigger if you have configured a lower power budget for that port and the port exceeds your configured budget.

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility pse-port <port-list> relay
no alarm facility pse-port <port-list> relay
```

Parameter	Description
<port-list>	The port or ports to monitor with this alarm. The port 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).

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use an alarm to flash the fault LED, by using the command alarm facility pse-port led.

Example To trigger the alarm relay if a PoE device plugged into port1.0.2 is consuming more than the maximum power output permitted for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility pse-port port1.0.2 relay
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility pse-port port1.0.2 relay
```

Related commands

alarm facility pse-port led

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches

alarm facility temperature led

Overview Use this command to make the fault LED flash if the switch's temperature goes above the high limit for any of its monitored temperature thresholds. To see the limits, use the command show system environment.

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility temperature led
no alarm facility temperature led
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use a relay to trigger an external alarm output, such as a buzzer, by using the command alarm facility temperature relay.

Example To flash the LED if the switch overheats, use the commands:

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

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility temperature led
```

Related commands

alarm facility temperature relay

show alarm facility settings

show alarm facility status

show system environment

Command changes Version 5.4.9-1.1: **input-member** and **output-member** parameters added on IE510-28GSX switches

alarm facility temperature relay

Overview Use this command to make the fault LED flash if the switch's temperature exceeds the high limit for any of its monitored temperature thresholds.

This will activate the device that you have connected to the switch's relay output (for example, you could connect a buzzer to the relay output).

To see the limits, use the command show system environment.

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility temperature relay
no alarm facility temperature relay
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use an alarm to flash the fault LED, by using the command alarm facility temperature led.

Example To trigger the alarm relay if the switch overheats, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility temperature relay
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility temperature relay
```

Related commands

alarm facility temperature led

show alarm facility settings

show alarm facility status

show system environment

Command changes Version 5.4.9-1.1: **input-member** and **output-member** parameters added on IE510-28GSX switches

alarm facility ufo led

Overview Use this command to make the fault LED flash if one or more UFO VLANs are isolated and cannot forward traffic.

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility ufo led
no alarm facility ufo led
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use a relay to trigger an external alarm output, such as a buzzer, by using the command alarm facility ufo relay.

Example To flash the LED if one or more UFO VLANs are isolated and cannot forward traffic, use the commands:

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

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility ufo led
```

Related commands alarm facility ufo relay

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches

alarm facility ufo relay

Overview Use this command to trigger an alarm relay if one or more UFO VLANs are isolated and cannot forward traffic.

This will activate the device that you have connected to the switch's relay output (for example, you could connect a buzzer to the relay output).

Use the **no** variant of this command to remove this alarm.

Syntax

```
alarm facility ufo relay
no alarm facility ufo relay
```

Default By default, there are no alarms

Mode Global Configuration

Usage notes You can also use an alarm to flash the fault LED, by using the command alarm facility ufo led.

Example To trigger the alarm relay if one or more UFO VLANs are isolated and cannot forward traffic, use the commands:

```
awplus# configure terminal
awplus(config)# alarm facility ufo relay
```

To remove that alarm, use the commands:

```
awplus# configure terminal
awplus(config)# no alarm facility ufo relay
```

Related commands alarm facility ufo led

show alarm facility settings

show alarm facility status

Command changes Version 5.4.9-1.1: **output-member** parameter added on IE510-28GSX switches

debug alarm

Overview Use this command to enable debugging of the Alarm Monitoring feature. When debugging is enabled, the switch displays debugging messages on the terminal monitor and in the log.

Use the **no** variant of this command to disable debugging of the Alarm Monitoring feature.

Syntax

```
debug alarm
no debug alarm
```

Default Disabled

Mode Global Configuration

Example To turn on Alarm debugging, use the commands:

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

Related commands show debugging alarm

show alarm facility settings

Overview Use this command to see whether an LED flashes or a relay is turned on if a certain alarm occurs. The output also includes the alarm position for each contact input.

Syntax
```
show alarm facility settings
```

Mode User Exec and Privileged Exec

Example To display all the alarm settings on a switch, use the following command:

```
awplus# show alarm facility settings
```

Output Figure 14-1: Example output from **show alarm facility settings**

```
awplus#show alarm facility settings

Global alarms:
Alarm                    ID           Outputs - L: LED, R: Relay
-------------------------------------------------------------------
EPSR                     -            -
Loop detect              -            -
G8032                    -            -
UFO                      -            -

Per stack member alarms:

Alarm                    ID           Outputs - L: LED, R: Relay
-------------------------------------------------------------------
External PSU             1            L
External PSU             2            L
External contact input   1            -
Link down                port1.0.1    R1
Link down                port1.0.2    -
Link down                port1.0.3    -
Link down                port1.0.4    -
...
Temperature              -            -

Alarm                    ID           Alarm position
-----------------------------------------------------
External contact input   1            Open
```

Related commands show alarm facility status

Command changes Version 5.4.9-1.1: command syntax changed from **show alarm settings** to **show alarm facility settings**

show alarm facility status

Overview Use this command to view alarms on the switch.

With the **all** parameter, the output lists all alarm sources that are currently in a fault state, even if there is no alarm configured for them.

Without the **all** parameter, the output only lists alarm sources that are currently in a fault state and have an alarm configured for them.

Syntax

```
show alarm facility status [all]
```

Parameter	Description
`all`	Display every alarm source that is in a fault state at this point of time.

Mode User Exec and Privileged Exec

Example To display the currently active alarms on the switch, use the command:

```
awplus# show alarm facility status
```

Output Figure 14-2: Example output from the **show alarm facility status** command

```
Active alarms            ID
-----------------------  ---------
External PSU             2
EPSR                     -
Link down                port1.0.1
```

Related commands show alarm facility settings

Command changes Version 5.4.9-1.1: command syntax changed from **show facility-alarm status** to **show alarm facility status**

show debugging alarm

Overview Use this command to see what debugging is turned on for Alarm Monitoring.

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

Syntax

```
show debugging alarm
```

Mode User Exec and Privileged Exec

Example To show the status of Alarm Monitoring debugging, use the command:

```
awplus# show debugging alarm
```

Output Figure 14-3: Example output from **show debugging alarm**

```
awplus#show debugging alarm

% Alarm debugging is disabled
```

Related commands debug alarm

Part 2: Interfaces and Layer 2

15 Switching Commands

Introduction

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

For more information, see the Switching Feature Overview and Configuration Guide.

Command List

- "backpressure" on page 540
- "clear loop-protection action" on page 542
- "clear loop-protection counters" on page 543
- "clear mac address-table dynamic" on page 544
- "clear mac address-table static" on page 546
- "clear port counter" on page 547
- "clear port-security intrusion" on page 548
- "cut-through" on page 550
- "debug loopprot" on page 551
- "debug platform packet" on page 552
- "duplex" on page 554
- "flowcontrol (switch port)" on page 555
- "linkflap action" on page 557
- "loop-protection loop-detect" on page 558
- "loop-protection action" on page 559
- "loop-protection action-delay-time" on page 560
- "loop-protection timeout" on page 561
- "mac address-table acquire" on page 562

- "mac address-table ageing-time" on page 563
- "mac address-table logging" on page 564
- "mac address-table static" on page 565
- "mac address-table thrash-limit" on page 566
- "platform hwfilter-size" on page 567
- "platform l3-vlan-hashing-algorithm" on page 568
- "platform load-balancing" on page 569
- "platform mac-vlan-hashing-algorithm" on page 570
- "platform multicast-ratelimit" on page 571
- "platform stop-unreg-mc-flooding" on page 572
- "platform vlan-stacking-tpid" on page 574
- "polarity" on page 575
- "show debugging loopprot" on page 576
- "show debugging platform packet" on page 577
- "show flowcontrol interface" on page 578
- "show interface err-disabled" on page 579
- "show interface switchport" on page 580
- "show loop-protection" on page 581
- "show mac address-table" on page 583
- "show mac address-table thrash-limit" on page 585
- "show platform" on page 586
- "show platform classifier statistics utilization brief" on page 589
- "show platform port" on page 591
- "show port-security interface" on page 593
- "show port-security intrusion" on page 594
- "show storm-control" on page 595
- "speed" on page 596
- "storm-control level" on page 598
- "switchport port-security" on page 599
- "switchport port-security aging" on page 601
- "switchport port-security maximum" on page 603
- "switchport port-security violation" on page 605
- "thrash-limiting" on page 607
- "undebug loopprot" on page 609
- "undebug platform packet" on page 610

backpressure

Overview This command provides a method of applying flow control to ports running in half duplex mode. The setting will only apply when the link is in the half-duplex state.

You can disable backpressure on an interface using the **off** parameter or the **no** variant of this command.

Syntax

```
backpressure {on|off}
no backpressure
```

Parameters	Description
`on`	Enables half-duplex flow control.
`off`	Disables half-duplex flow control.

Default Backpressure is turned off by default. You can determine whether an interface has backpressure enabled by viewing the running-config output; **backpressure on** is shown for interfaces if this feature is enabled.

Mode Interface Configuration

Usage notes The backpressure feature enables half duplex Ethernet ports to control traffic flow during congestion by preventing further packets arriving. Backpressure utilizes a pre-802.3x mechanism in order to apply Ethernet flow control to switch ports that are configured in the half duplex mode.

The flow control applied by the flowcontrol (switch port) command operates only on full-duplex links, whereas backpressure operates only on half-duplex links.

If a port has insufficient capacity to receive further frames, the device will simulate a collision by transmitting a CSMACD jamming signal from this port until the buffer empties. The jamming signal causes the sending device to stop transmitting and wait a random period of time, before retransmitting its data, thus providing time for the buffer to clear. Although this command is only valid for switch ports operating in half-duplex mode the remote device (the one sending the data) can be operating in the full duplex mode.

To see the currently-negotiated duplex mode for ports whose links are up, use the command show interface. To see the configured duplex mode (when different from the default), use the command show running-config.

Examples To enable backpressure flow control on port1.0.2, enter the following commands:

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

To disable backpressure flow control on interface port1.0.2, enter the following commands:

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

Related commands

duplex

show interface

show running-config

clear loop-protection action

Overview Use this command to clear the loop protection actions on the specified interfaces.

Syntax

```
clear loop-protection [interface <port-list>] action
```

Parameters	Description
`interface`	The interface whose actions are to be cleared.
<port-list>	A port, a port range, or an aggregated link.

Mode Privileged Exec

Example To clear the loop protection actions on interface port1.0.2, use the command:

```
awplus# clear loop-protection interface port1.0.2 action
```

To clear the loop protection actions of all interfaces on a device, use the command:

```
awplus# clear loop-protection action
```

Related commands

loop-protection loop-detect

loop-protection action

show loop-protection

clear loop-protection counters

Overview Use this command to clear the loop protection counters.

Syntax

```
clear loop-protection [interface <port-list>] counters
```

Parameters	Description
`interface`	The interface whose counters are to be cleared.
<port-list>	A port, a port range, or an aggregated link.

Mode Privileged Exec

Examples To clear the counter information for all interfaces:

```
awplus# clear loop-protection counters
```

To clear the counter information for a single port:

```
awplus# clear loop-protection interface port1.0.1 counters
```

Related commands show loop-protection

clear mac address-table dynamic

Overview Use this command to clear the filtering database of all entries learned for a selected MAC address, an MSTP instance, a switch port interface, or a VLAN interface.

Syntax

```
clear mac address-table dynamic
[address <mac-address>|interface <port> [instance <inst>]|
vlan <vid>]
```

Parameter	Description
`address <mac-address>`	Specify a MAC (Media Access Control) address to be cleared from the filtering database, in the format HHHH.HHHH.HHHH.
`interface <port>`	Specify a switch port to be cleared from the filtering database. The port can be: • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2)
`instance <inst>`	Specify an MSTP (Multiple Spanning Tree) instance in the range 1 to 63 to be cleared from the filtering database.
`vlan <vid>`	Specify a VID (VLAN ID) in the range 1 to 4094 to be cleared from the filtering database.

Mode Privileged Exec

Usage notes Use this command with options to clear the filtering database of all entries learned for a given MAC address, interface or VLAN. Use this command without options to clear any learned entries.

Use the optional **instance** parameter to clear the filtering database entries associated with a specified MSTP instance. Note that you must first specify a switch port interface before you can specify an MSTP instance.

Compare this usage and operation with the clear mac address-table static command. Note that an MSTP instance cannot be specified with the command **clear mac address-table static**.

Examples This example shows how to clear all dynamically learned filtering database entries.

```
awplus# clear mac address-table dynamic
```

This example shows how to clear all dynamically learned filtering database entries when learned through device operation for the MAC address 0000.5E00.5302.

```
awplus# clear mac address-table dynamic address 0000.5E00.5302
```

This example shows how to clear all dynamically learned filtering database entries when learned through device operation for a given MSTP instance 1 on switch port interface port1.0.3.

```
awplus# clear mac address-table dynamic interface port1.0.3
instance 1
```

Related commands

clear mac address-table static

show mac address-table

clear mac address-table static

Overview Use this command to clear the filtering database of all statically configured entries for a selected MAC address, interface, or VLAN.

Syntax

```
clear mac address-table static [address <mac-address>|interface
<port>|vlan <vid>]
```

Parameter	Description
`address <mac-address>`	Specify a MAC (Media Access Control) address to be cleared from the filtering database, in the format HHHH.HHHH.HHHH.
`interface <port>`	Specify the port from which statically configured entries are to be cleared. The port can be • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2)
`vlan <vid>`	Specify a VID (VLAN ID) in the range 1 to 4094 to be cleared from the filtering database.

Mode Privileged Exec

Usage notes Use this command with options to clear the filtering database of all entries made from the CLI for a given MAC address, interface or VLAN. Use this command without options to clear any entries made from the CLI.

Compare this usage with clear mac address-table dynamic command.

Examples This example shows how to clear all filtering database entries configured through the CLI.

```
awplus# clear mac address-table static
```

This example shows how to clear all filtering database entries for a specific interface configured through the CLI.

```
awplus# clear mac address-table static interface port1.0.3
```

This example shows how to clear filtering database entries configured through the CLI for the MAC address 0000.5E00.5302.

```
awplus# clear mac address-table static address 0000.5E00.5302
```

Related commands

clear mac address-table dynamic

mac address-table static

show mac address-table

clear port counter

Overview Use this command to clear the packet counters of the port.

Syntax

```
clear port counter [<port>]
```

Parameter	Description
<port>	The port number or range

Mode Privileged Exec

Example To clear the packet counter for port1.0.1, use the command:

```
awplus#  clear port counter port1.0.1
```

Related commands show platform port

clear port-security intrusion

Overview Use this command to clear the history of the port-security intrusion list on all ports, or an individual port. If you do not specify a port, this command clears the intrusion lists of all ports.

This command does not clear any MAC addresses the switch has already learned. If you want to clear already-learned MAC addresses from the filtering database, use the clear mac address-table dynamic command or the clear mac address-table static command.

Syntax

```
clear port-security intrusion [interface <port>]
```

Parameter	Description
<port>	Specify the switch port from which the history of violated address entries will be cleared, e.g. port1.0.4.

Mode Privileged Exec

Examples To see the intrusion list on port1.0.2, use the following command:

```
awplus# show port-security intrusion interface port1.0.2
```

Table 15-1: Example output from **show port-security intrusion**

```
awplus#show port-security intrusion interface port1.0.2
Port Security Intrusion List
------------------------------------------------------------
Interface: port1.0.2     - 1 intrusion(s) detected
801f.0200.19da
```

To clear the history of port-security intrusion list on port1.0.2, use the following command:

```
awplus# clear port-security intrusion interface port1.0.2
```

To see the port-security status on port1.0.2, use the following command:

```
awplus# show port-security interface port1.0.2
```

Table 15-2: Example output from **show port-security interface**

```
awplus#show port-security interface port1.0.2
Port Security configuration
------------------------------------------------------------
Security Enabled : YES
Port Status : ENABLED
Violation Mode : TRAP
Aging : OFF
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Lock Status : LOCKED
Security Violation Count : 0
Last Violation Source Address : None
```

NOTE: *Note that the port status is still locked while the history of port violation is cleared from the database.*

To re-check the intrusion list on port1.0.2, use the following command:

```
awplus# show port-security intrusion interface port1.0.2
```

Table 15-3: Example output from **show port-security intrusion**

```
awplus#show port-security intrusion interface port1.0.2
Port Security Intrusion List
------------------------------------------------------------
Interface: port1.0.2     - no intrusions detected
```

Related commands

show port-security interface

show port-security intrusion

switchport port-security

switchport port-security aging

switchport port-security maximum

switchport port-security violation

Command changes

Version 5.5.1-0.1: port-security on LAGs added for SBx81CFC960, SBx908 GEN2, x950, x930, x550, x530, x530L, x320, x230, x230L and x220 Series switches

cut-through

Overview This command changes the switching method setting to the cut-through switching method on the specified port.

Use the `no` variant of this command to restore the switching method setting to the default store-and-forward switching method on the specified port.

Syntax

```
cut-through
no cut-through
```

Default The store-and forward switching method

Mode Interface Configuration for a switch port interface

Usage Use this command to change the switching method setting to cut-through switching on a port.

In store-and-forward switching, the switch stores the entire frame in the buffers and performs error checking before forwarding the frame. In cut-through switching, the switch forwards a frame without waiting to receive the entire frame. Because the switch does not wait for the entire frame to receive, nor perform error checking, cut-through switching is faster than store-and-forward switching.

To make the link operate in the cut-through method, both egress and ingress ports must be set to the cut-through method using the **cut-through** command. In addition, if the ingress port speed is slower than the egress port speed, the link between the two ports operates in the store-and-forward method.

Examples To change the switching method on port1.0.1 to port1.0.8 to cut-through switching, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.8
awplus(config-router)# cut-through
```

To change the switching method to store-and-forward switching, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.8
awplus(config-router)# no cut-through
```

Related Command show running-config

debug loopprot

Overview This command enables Loop Protection debugging.

The **no** variant of this command disables Loop Protection debugging.

Syntax

```
debug loopprot {info|msg|pkt|state|nsm|all}
no debug loopprot {info|msg|pkt|state|nsm|all}
```

Parameter	Description
`info`	General Loop Protection information.
`msg`	Received and transmitted Loop Detection Frames (LDFs).
`pkt`	Echo raw ASCII display of received and transmitted LDF packets to the console.
`state`	Loop Protection states transitions.
`nsm`	Network Service Module information.
`all`	All debugging information.

Mode Privileged Exec and Global Configuration

Example To enable debug for all state transitions, use the command:

```
awplus#  debug loopprot state
```

Related commands show debugging loopprot

undebug loopprot

debug platform packet

Overview This command enables platform to CPU level packet debug functionality on the device.

Use the **no** variant of this command to disable platform to CPU level packet debug. If the result means both send and receive packet debug are disabled, then any active timeout will be canceled.

Syntax

```
debug platform packet [recv] [send] [sflow] [timeout <timeout>]
[vlan <vid>|all]
```

```
no debug platform packet [recv] [send]
```

Parameter	Description
`recv`	Debug packets received.
`send`	Debug packets sent.
`sflow`	Debug sFlow packets.
`timeout <timeout>`	Stop debug after a specified time. Specify the time in seconds.
`vlan <vid>`	Specify a VID (VLAN ID) in the range 1 to 4094 to limit debug to that VLAN.
`all`	Debug all VLANs (default setting).

Default A 5 minute timeout is configured by default if no other timeout duration is specified.

Mode Privileged Exec and Global Configuration

Usage notes This command can be used to trace packets sent and received by the CPU. If a timeout is not specified, then a default 5 minute timeout will be applied.

If a timeout of 0 is specified, packet debug will be generated until the **no** variant of this command is used or another timeout value is specified. The timeout value applies to both send and receive debug and is updated whenever the **debug platform packet** command is used.

Examples To enable both receive and send packet debug for the default timeout of 5 minutes, enter:

```
awplus# debug platform packet
```

To enable receive packet debug for 10 seconds, enter:

```
awplus# debug platform packet recv timeout 10
```

To enable packet debug for sFlow packets only for the default timeout of 5 minutes, enter:

```
awplus# debug platform packet sflow
```

To enable send packet debug with no timeout, enter:

```
awplus# debug platform packet send timeout 0
```

To enable VLAN packet debug for VLAN 1 with a timeout duration of 3 minutes, enter:

```
awplus# debug platform packet vlan 1 timeout 180
```

To disable receive packet debug, enter:

```
awplus# no debug platform packet recv
```

Related commands

show debugging platform packet

undebug platform packet

duplex

Overview This command changes the duplex mode for the specified port.

To see the currently-negotiated duplex mode for ports whose links are up, use the command show interface. To see the configured duplex mode (when different from the default), use the command show running-config.

Syntax

```
duplex {auto|full|half}
```

Parameter	Description
`auto`	Auto-negotiate duplex mode.
`full`	Operate in full duplex mode only.
`half`	Operate in half duplex mode only.

Default By default, ports auto-negotiate duplex mode (except for 100Base-FX ports which do not support auto-negotiation, so default to full duplex mode).

Mode Interface Configuration

Usage notes Switch ports in a static or dynamic (LACP) channel group must have the same port speed and be in full duplex mode. Once switch ports have been aggregated into a channel group, you can set the duplex mode of all the switch ports in the channel group by applying this command to the channel group.

Examples To specify full duplex for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex full
```

To specify half duplex for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex half
```

To auto-negotiate duplex mode for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex auto
```

Related commands

polarity

speed

show interface

flowcontrol (switch port)

Overview Use this command to enable flow control, and configure the flow control mode for the switch port.

Use the **no** variant of this command to disable flow control for the specified switch port.

Syntax

```
flowcontrol {receive|send} {off|on}
no flowcontrol
```

Parameter	Description
`receive`	When the port receives pause frames, it temporarily stops (pauses) sending traffic.
`send`	When the port is congested (receiving too much traffic), it sends pause frames to request the other end to temporarily stop (pause) sending traffic.
`on`	Enable the specified flow control.
`off`	Disable the specified flow control.

Default By default, flow control is disabled.

Mode Interface Configuration

Usage notes The flow control mechanism specified by 802.3x is only for full duplex links. It operates by sending PAUSE frames to the link partner to temporarily suspend transmission on the link.

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion, and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When the local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the congestion period.

Flow control is not recommended when running QoS or ACLs, because the complex queuing, scheduling, and filtering configured by QoS or ACLs may be slowed by applying flow control.

For half-duplex links, an older form of flow control known as backpressure is supported. See the related backpressure command.

For flow control on async serial (console) ports, see the flowcontrol hardware (asyn/console) command.

Examples

To enable flow control on port1.0.2 (receive only), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol receive on
```

To enable flow control on port1.0.2 (send only), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol send on
```

To disable flow control on port1.0.2 (receive only), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol receive off
```

To disable flow control on port1.0.2 (send only), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol send off
```

Related commands

backpressure

show running-config

linkflap action

Overview Use this command to detect flapping on all ports. If more than 15 flaps occur in less than 15 seconds the flapping port will shut down.

Use the **no** variant of this command to disable flapping detection at this rate.

Syntax

```
linkflap action [shutdown]
no linkflap action
```

Parameter	Description
`linkflap`	Global setting for link flapping.
`action`	Specify the action for port.
`shutdown`	Shutdown the port.

Default Linkflap action is disabled by default.

Mode Global Configuration

Example To enable the linkflap action command on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# linkflap action shutdown
```

loop-protection loop-detect

Overview Use this command to enable the loop-protection loop-detect feature and configure its parameters.

Use the **no** variant of this command to disable the loop-protection loop-detect feature.

Syntax

```
loop-protection loop-detect [ldf-interval <period>]
[ldf-rx-window <frames>] [fast-block]
```

```
no loop-protection loop-detect
```

Parameter	Description
`ldf-interval`	The time (in seconds) between successive loop-detect frames being sent.
<period>	Specify a period between 1 and 600 seconds. The default is 10 seconds.
`ldf-rx-window`	The number of transmitted loop detect frames whose details are held for comparing with frames arriving at the same port.
<frames>	Specify a value for the window size between 1 and 5 frames. The default is 3 frames.
`[fast-block]`	The fast-block blocks transmitting port to keep partial connectivity.

Default The loop-protection loop-detect feature is disabled by default. The default interval is 10 seconds, and the default window size is 3 frames.

Mode Global Configuration

Usage notes See the "Loop Protection" section in the Switching Feature Overview and Configuration Guide for relevant conceptual, configuration, and overview information prior to applying this command.

Example To enable the loop-detect mechanism on the switch, and generate loop-detect frames once every 5 seconds, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# loop-protection loop-detect ldf-interval 5
```

Related commands

loop-protection action

loop-protection timeout

show loop-protection

loop-protection action

Overview Use this command to specify the protective action to apply when a network loop is detected on an interface.

Use the **no** variant of this command to reset the loop protection actions to the default action, vlan-disable, on an interface.

Syntax

```
loop-protection action
{link-down|log-only|port-disable|vlan-disable|none}
```

```
no loop-protection action
```

Parameter	Description
`link-down`	Block all traffic on a port (or aggregated link) that detected the loop, and take **down** the link.
`log-only`	Details of loop conditions are logged. No action is applied to the port (or aggregated link).
`port-disable`	Block all traffic on interface for which the loop occurred, but keep the link in the **up** state.
`vlan-disable`	Block all traffic for the VLAN on which the loop traffic was detected. Note that setting this parameter will also enable ingress filtering. This is the default action.
`none`	Applies no protective action.

Default loop-protection action vlan-disable

Mode Interface Configuration

Usage notes See the "Loop Protection" section in the Switching Feature Overview and Configuration Guide for relevant conceptual, configuration, and overview information prior to applying this command.

Example To disable the interface `port1.0.2` and bring the link down when a network loop is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# loop-protection action link-down
```

Related commands

loop-protection loop-detect

loop-protection timeout

show loop-protection

loop-protection action-delay-time

Overview Use this command to sets the loop protection action delay time for an interface to specified values in seconds. The action delay time specifies the waiting period for the action.

Use the **no** variant of this command to reset the loop protection action delay time for an interface to default.

Syntax

```
loop-protection action-delay-time <0-86400>
no loop-protection action
```

Parameter	Description
<0-86400>	Time in seconds; 0 means action delay timer is disabled.

Default Action delay timer is disabled by default.

Mode Interface Configuration

Example To configure a loop protection action delay time of 10 seconds on port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection action-delay-time 10
```

Related commands

loop-protection loop-detect

loop-protection timeout

show loop-protection

loop-protection timeout

Overview Use this command to specify the Loop Protection recovery action duration on an interface.

Use the **no** variant of this command to set the loop protection timeout to the default.

Syntax

```
loop-protection timeout <duration>
no loop-protection timeout
```

Parameter	Description
<duration>	The time (in seconds) for which the configured action will apply before being disabled. This duration can be set between 0 and 86400 seconds (24 hours). The set of 0 means infinity so timeout does not expire.

Default The default is 7 seconds.

Mode Interface Configuration

Usage notes See the "Loop Protection" section in the Switching_Feature Overview_and Configuration_Guide for relevant conceptual, configuration, and overview information prior to applying this command.

Example To configure a loop protection action timeout of 10 seconds for port1.0.4, use the command:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection timeout 10
```

Related commands

loop-protection loop-detect

loop-protection action

show loop-protection

mac address-table acquire

Overview Use this command to enable MAC address learning on the device.

Use the **no** variant of this command to disable learning.

Syntax
```
mac address-table acquire
no mac address-table acquire
```

Default Learning is enabled by default for all instances.

Mode Global Configuration

Example
```
awplus# configure terminal
awplus(config)# mac address-table acquire
```

mac address-table ageing-time

Overview Use this command to specify an ageing-out time for a learned MAC address. The learned MAC address will persist for at least the specified time.

The **no** variant of this command will reset the ageing-out time back to the default of 300 seconds (5 minutes).

Syntax

```
mac address-table ageing-time <ageing-timer> none
no mac address-table ageing-time
```

Parameter	Description
<ageing-timer>	*<10-1000000>* The number of seconds of persistence.
none	Disable learned MAC address timeout.

Default The default ageing time is 300 seconds.

Mode Global Configuration

Examples The following commands specify various ageing timeouts on the device:

```
awplus# configure terminal
awplus(config)# mac address-table ageing-time 1000
awplus# configure terminal
awplus(config)# mac address-table ageing-time none
awplus# configure terminal
awplus(config)# no mac address-table ageing-time
```

mac address-table logging

Overview Use this command to create log entries when the content of the FDB (forwarding database) changes. Log messages are produced when a MAC address is added to or removed from the FDB.

CAUTION: *MAC address table logging may impact the performance of the switch. Only enable it when necessary as a debug tool.*

Use the **no** variant of this command to stop creating log entries when the content of the FDB changes.

Syntax

```
mac address-table logging
no mac address-table logging
```

Default MAC address table logging is disabled by default.

Mode User Exec/Privileged Exec

Usage When MAC address table logging is enabled, the switch produces the following messages:

Change	Message format	Example
MAC added	MAC add <*mac*> <*port*> <*vlan*>	MAC add eccd.6db5.68a7 port1.0.1 vlan2
MAC removed	MAC remove <*mac*> <*port*> <*vlan*>	MAC remove eccd.6db5.68a7 port1.0.1 vlan2

Note that rapid changes may not be logged. For example, if an entry is added and then removed within a few seconds, those actions may not be logged.

To see whether MAC address table logging is enabled, use the command show running-config.

Example To create log messages when the content of the FDB changes, use the command:

```
awplus# mac address-table logging
```

Related commands show running-config

mac address-table static

Overview Use this command to statically configure the MAC address-table to forward or discard frames with a matching destination MAC address.

Syntax

```
mac address-table static <mac-addr> {forward|discard} interface
<port> [vlan <vid>]
```

```
no mac address-table static <mac-addr> {forward|discard}
interface <port> [vlan <vid>]
```

Parameter	Description
<mac-addr>	The destination MAC address in `HHHH.HHHH.HHHH` format.
`interface` *<port>*	Specify a switch port to be cleared from the filtering database. The port can be: • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2)
`vlan` *<vid>*	The ID of a VLAN to apply the command to, in the range 1 to 4094. If you do not specify a VLAN, the command applies to VLAN1.

Mode Global Configuration

Usage notes The **mac address-table static** command is only applicable to Layer 2 switched traffic within a single VLAN. Do not apply the **mac address-table static** command to Layer 3 switched traffic passing from one VLAN to another VLAN. Frames will not be discarded across VLANs because packets are routed across VLANs. This command only works on Layer 2 traffic.

Example

```
awplus# configure terminal
```

```
awplus(config)# mac address-table static 2222.2222.2222 forward
interface port1.0.4 vlan 3
```

Related commands clear mac address-table static

show mac address-table

mac address-table thrash-limit

Overview Use this command to set the thrash limit on the device.

Thrashing occurs when a MAC address table rapidly "flips" its mapping of a single MAC address between two switchports on the same VLAN. This is usually because of a network loop.

Use the **no** variant of this command to return the thrash limit to its default setting.

Syntax

```
mac address-table thrash-limit <rate>
no mac address-table thrash-limit
```

Parameter	Description
<rate>	The maximum thrash rate at which limiting is applied. This rate can be set to between 5 and 255 MAC thrashing flips per second. Once the thrash limit rate is reached, the port is considered to be thrashing.

Default 10 MAC thrashing flips per second

Mode Global Configuration

Usage notes Use this command to limit thrashing on the selected port range.

Example To apply a thrash limit of 20 MAC address flips per second:

```
awplus# configure terminal
awplus(config)# mac address-table thrash-limit 20
```

Related commands

show interface

show mac address-table thrash-limit

thrash-limiting

platform hwfilter-size

Overview You can use this command to control the configuration of hardware Access Control Lists (ACLs), which determines the total available number and functionality of hardware ACLs.

For this command to take effect, you need to reboot the affected service.

You cannot attach an IPv6 ACL to a port if the ACL contains a specified source or destination IPv6 address or both and the **hw-filter size** setting is **ipv4-limited-ipv6**. If you do so, a diagnostic message will be generated.

Syntax

```
platform hwfilter-size {ipv4-limited-ipv6|ipv4-full-ipv6}
```

Parameter	Description
`hwfilter-size`	Configure hardware ACLs command.
`ipv4-full-ipv6`	Configure hardware ACLs to filter IPv4 traffic, MAC addresses and IPv6 traffic, including filtering on source or destination IPv6 addresses, or both; however, this will reduce the total number of filters available in the hardware table.
`ipv4-limited-ipv6`	Configure hardware ACLs to filter IPv4 traffic, MAC addresses and IPv6 traffic. Source or destination IPv6 addresses or both are not filtered.

Default The default mode is **ipv4-limited-ipv6**.

Mode Global Configuration

Example To configure hardware ACLs to filter IPv4 and IPv6 traffic, use the following commands:

```
awplus# configure terminal
awplus(config)# platform hwfilter-size ipv4-full-ipv6
```

Related commands show platform

ipv6 access-list (named IPv6 hardware ACL)

platform l3-vlan-hashing-algorithm

Overview This command enables you to change the L3 VLAN hash-key-generating algorithm.

The **no** variant of this command returns the hash-key algorithm to the default of crc32l.

Syntax

```
platform l3-vlan-hashing-algorithm
{crc16l|crc16u|crc32l|crc32u}
```

```
no platform l3-vlan-hashing-algorithm
```

Parameter	Description
`crc16l`	The algorithm that will apply to the lower bits of CRC-16
`crc16u`	The algorithm that will apply to the upper bits of CRC-16
`crc32l`	The algorithm that will apply to the lower bits of CRC-32
`crc32u`	The algorithm that will apply to the upper bits of CRC-32

Default The hash-key algorithm is crc32l by default.

Mode Global configuration

Usage notes Occasionally, when using the Multiple Dynamic VLAN feature, a supplicant cannot be authenticated because a collision occurs within the VLAN L3 table. This can happen when more than four different IP addresses produce the same hash-key.

When this situation occurs, collisions can sometimes be avoided by changing the hashing algorithm from its default of crc32l. Several different algorithms may need to be tried to rectify the problem.

You must restart the switch for this command to take effect.

Note that this command is intended for technical support staff, or advanced end users.

Example To change the hash-key generating algorithm applying to the lower bits of CRC-16, use the command:

```
awplus# configure terminal
awplus(config)# platform l3-vlan-hashing-algorithm crc16l
```

Related commands platform mac-vlan-hashing-algorithm

show platform

platform load-balancing

Overview This command selects which address fields are used as inputs into the load balancing algorithm for aggregated links. The output from this algorithm is used to select which individual path a given packet will traverse within an aggregated link.

The **no** variant of this command applies its default setting.

Syntax

```
platform load-balancing {src-dst-mac|src-dst-ip}
no platform load-balancing
```

Parameter	Description
`src-dst-mac`	Include the source and destination MAC addresses (Layer 2)
`src-dst-ip`	Include the source and destination IP addresses (Layer 3) and UDP/TCP source and destination ports. If you choose this option, the algorithm will use MAC addresses to calculate load balancing for Layer 2 and non-IP packets.

Default The default is **src-dst-ip**.

Mode Global configuration

Examples To set the load balancing algorithm to include only Layer 2 MAC addresses, use the commands:

```
awplus# configure terminal
awplus(config)# platform load-balancing src-dst-mac
```

To set the load balancing algorithm to include only Layer 3 IP addresses and Layer 4 ports, use the commands:

```
awplus# configure terminal
awplus(config)# platform load-balancing src-dst-ip
```

Related commands show platform

platform mac-vlan-hashing-algorithm

Overview This command enables you to change the MAC VLAN hash-key-generating algorithm.

The **no** variant of this command returns the hash-key algorithm to the default of crc32l

Syntax

```
platform mac-vlan-hashing-algorithm
{crc16l|crc16u|crc32l|crc32u}
```

```
no platform mac-vlan-hashing-algorithm
```

Parameter	Description
`crc16l`	The algorithm that will apply to the lower bits of CRC-16
`crc16u`	The algorithm that will apply to the upper bits of CRC-16
`crc32l`	The algorithm that will apply to the lower bits of CRC-32
`crc32u`	The algorithm that will apply to the upper bits of CRC-32

Default The hash-key algorithm is crc32l by default.

Mode Global configuration

Usage notes Occasionally, when using the Multiple Dynamic VLAN feature, a supplicant cannot be authenticated because a collision occurs within the VLAN MAC table. This can happen when more than four different MAC addresses produce the same hash-key.

When this situation occurs, collisions can sometimes be avoided by changing the hashing algorithm from its default of crc32l. Several different algorithms may need to be tried to rectify the problem.

You must restart the switch for this command to take effect.

Note that this command is intended for technical support staff, or advanced end users.

Example To change the hash-key generating algorithm applying to the lower bits of CRC-16, use the command:

```
awplus# configure terminal
awplus(config)# platform mac-vlan-hashing-algorithm crc16l
```

Related commands platform l3-vlan-hashing-algorithm

show platform

platform multicast-ratelimit

Overview Use this command to set the maximum number of multicast packets to be forwarded to the CPU (in packets per second). Setting the value to zero disables rate limiting.

This command should be used with care. Increasing or removing the limit could make the device less responsive under heavy multicast load.

Use the **no** variant of this command to return the limit to its default.

Syntax

```
platform multicast-ratelimit <0-1000>
no platform multicast-ratelimit
```

Default 10 packets per second (pps)

Mode Global Configuration

Usage notes If you find that the CPU load on your device from multicast traffic is higher than desired, reducing this rate may reduce the CPU load.

If you need the device to process a large amount of multicast traffic, increasing this rate may improve performance.

Example To set the rate to 30pps, use the commands:

```
awplus# configure terminal
awplus(config)# platform multicast-ratelimit 30
```

Command changes Version 5.4.8-1.1: default changed to 100pps on SBx908 GEN2, SBx8100, and x930 Series switches.

platform stop-unreg-mc-flooding

Overview If a multicast stream is arriving at a network device, and that network device has received no IGMP reports that request the receipt of the stream, then that stream is referred to as "unregistered". IGMP snooping actively prevents the flooding of unregistered streams to all ports in the VLAN on which the stream is received. However, there are brief moments at which this prevention is not in operation, and an unregistered stream may be briefly flooded. This command stops this flooding during even those brief periods when IGMP snooping is not explicitly preventing the flooding.

Use the **no** variant of this command to revert to default behavior and disable this feature.

NOTE: *This command should not be used within any IPv6 networks. IPv6 neighbor discovery operation is inhibited by this feature.*

This command does not affect the flooding of Local Network Control Block IPv4 multicast packets in the address range 224.0.0.1 to 224.0.0.255 (224.0.0/24). Such packets will continue to be uninterruptedly flooded, as they need to be.

Syntax

```
platform stop-unreg-mc-flooding
no platform stop-unreg-mc-flooding
```

Default This feature is disabled by default.

Mode Global Configuration

Usage notes This command stops the periodic flooding of unknown or unregistered multicast packets when the Group Membership interval timer expires and there are no subscribers to a multicast group. If there is multicast traffic in a VLAN without subscribers, multicast traffic temporarily floods out of the VLAN when the Group Membership interval timer expires, which happens when the switch does not get replies from Group Membership queries.

This command also stops the initial flood of multicast packets that happens when a new multicast source starts to send traffic. This flooding lasts until snooping realises that this the multicast group is arriving at the switch, and puts an entry into hardware to prevent it from being flooded.

This command is useful in networks where low-performance devices are attached. The operation of such devices can be impaired by them receiving unnecessary streams of traffic. For example, in sites where IP cameras are in use, the flooding of video streams to a whole VLAN can send enough traffic to the cameras to cause interruption of their video streaming.

Do not use this command in IPv6 networks. The following console message is displayed after entering this command to warn you of this:

```
% WARNING: IPv6 will not work with this setting enabled
% Please consult the documentation for more information
```

Examples

To enable this feature and stop multicast packet flooding, use the following commands:

```
awplus# configure terminal
awplus(config)# platform stop-unreg-mc-flooding
```

To disable this feature and allow multicast packet flooding, use the following commands:

```
awplus# configure terminal
awplus(config)# no platform stop-unreg-mc-flooding
```

Related commands

show platform

show running-config

platform vlan-stacking-tpid

Overview This command specifies the Tag Protocol Identifier (TPID) value that applies to all frames that are carrying double tagged VLANs. All such VLANs must use the same TPID value. (This feature can be referred to as nested VLANs, VLAN stacking, Q-in-Q, or VLAN double-tagging.)

Use the **no** variant of this command to revert to the default TPID value (0x8100).

NOTE: *Because the additional tag increases the frame size beyond 1522 bytes, you must increase the MRU size to activate VLAN-stacking. Go into interface mode for the appropriate ports and use the mru command.*

Syntax

```
platform vlan-stacking-tpid <tpid>
no platform vlan-stacking-tpid
```

Parameter	Description
<tpid>	The Ethernet type of the tagged packet, as a two byte hexadecimal number.

Default The default TPID value is 0x8100.

Mode Global Configuration

Examples To set the VLAN stacking TPID value to 0x9100, use the following commands:

```
awplus# configure terminal
awplus(config)# platform vlan-stacking-tpid 9100
```

To reset the VLAN stacking TPID value to the default (0x8100), use the following commands:

```
awplus# configure terminal
awplus(config)# no platform vlan-stacking-tpid
```

Related commands

switchport vlan-stacking (double-tagging)

show platform

show running-config

polarity

Overview This command sets the MDI/MDIX polarity on a copper-based switch port.

Syntax

```
polarity {auto|mdi|mdix}
```

Parameter	Description
`mdi`	Sets the polarity to MDI (medium dependent interface).
`mdix`	Sets the polarity to MDI-X (medium dependent interface crossover).
`auto`	The switch port sets the polarity automatically. This is the default option.

Default By default, switch ports set the polarity automatically (**auto**).

Mode Interface Configuration

Usage notes We recommend the default **auto** setting for MDI/MDIX polarity. Polarity applies to copper 10BASE-T, 100BASE-T, and 1000BASE-T switch ports; it does not apply to fiber ports. See the "MDI/MDIX Connection Modes" section in the Switching Feature Overview and Configuration Guide for more information.

Example To set the polarity for port1.0.4 to fixed MDI mode, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# polarity mdi
```

show debugging loopprot

Overview This command shows Loop Protection debugging information.

Syntax

```
show debugging loopprot
```

Mode User Exec and Privileged Exec

Example To display the enabled Loop Protection debugging modes, use the command:

```
awplus# show debugging loopprot
```

Related commands debug loopprot

show debugging platform packet

Overview This command shows platform to CPU level packet debugging information.

Syntax

```
show debugging platform packet
```

Mode User Exec and Privileged Exec

Example To display the platform packet debugging information, use the command:

```
awplus# show debugging platform packet
```

Related commands debug platform packet

undebug platform packet

show flowcontrol interface

Overview Use this command to display flow control information.

Syntax

```
show flowcontrol interface <port>
```

Parameter	Description
<port>	Specifies the name of the port to be displayed.

Mode User Exec and Privileged Exec

Example To display the flow control for port1.0.3, use the command:

```
awplus# show flowcontrol interface port1.0.3
```

Output Figure 15-1: Example output from the **show flowcontrol interface** command for a specific interface

```
Port      Send  FlowControl    Receive  FlowControl  RxPause TxPause
          admin    oper         admin    oper
-----     ------- --------     ------- --------     ------- -------
port1.0.3 on       on           on       on           0       0
```

show interface err-disabled

Overview Use this command to show the ports which have been dynamically shut down by protocols running on the device and the protocols responsible for the shutdown.

Syntax `show interface [<interface-range> err-disabled]`

Parameter	Description
<interface-range>	Interface range
`err-disabled`	Brief summary of interfaces shut down by protocols

Mode User Exec and Privileged Exec

Example To show which protocols have shut down ports, use the commands:

```
awplus# show interface err-disabled
```

Output Figure 15-2: Example output from **show interface err-disabled**

```
awplus#show interface err-disabled
Interface            Reason
port1.0.1            loop protection
port1.0.2            loop protection
```

show interface switchport

Overview Use this command to show VLAN information about each switch port.

Syntax

```
show interface switchport
```

Mode User Exec and Privileged Exec

Example To display VLAN information about each switch port, enter the command:

```
awplus# show interface switchport
```

Output Figure 15-3: Example output from the **show interface switchport** command

```
 Interface name          : port1.0.1
 Switchport mode         : access
 Ingress filter          : enable
 Acceptable frame types  : all
 Default Vlan            : 1
 Configured Vlans        : 2
 Dynamic Vlans           :

 Interface name          : port1.0.2
 Switchport mode         : trunk
 Ingress filter          : enable
 Acceptable frame types  : all
 Default Vlan            : 1
 Configured Vlans        : 1 4 5 6 7 8
 Dynamic Vlans           :
...
```

Related commands show interface memory

show loop-protection

Overview Use this command to display the current loop protection setup for the device.

Syntax

```
show loop-protection [interface <port-list>] [counters]
```

Parameter	Description
`interface`	The interface selected for display.
<port-list>	A port, a port range, or an aggregated link.
`counters`	Displays counter information for loop protection.

Mode User Exec and Privileged Exec

Usage notes This command is used to display the current configuration and operation of the Loop Protection feature.

Example To display the current configuration status, use the command:

```
awplus# show loop-protection
```

Output Figure 15-4: Example output from the **show loop-protection** command:

```
awplus#show loop-protection

LDF Interval:       10
Fast Block:   Disabled
                                                        Timeout
  Int           Enabled  Action     Status    Timeout   Remain   Rx port
  ------------------------------------------------------------------------
  port1.0.1     Yes      vlan-dis   Normal    7         -        -
  port1.0.2     Yes      vlan-dis   Normal    7         -        -
  port1.0.3     Yes      vlan-dis   Normal    7         -        -
...
```

Example To display the counter information, use the command:

```
awplus# show loop-protection counters
```

Output Figure 15-5: Example output from the **show loop-protection counters** command:

```
awplus#show loop-protection counters

Switch Loop Detection Counter

  Interface     Tx         Rx        Rx Invalid     Last LDF Rx
  ------------------------------------------------------------------------
  port1.0.1
      vlan1     60         0         0              -
  port1.0.2
      vlan1     0          0         0              -
  port1.0.3
      vlan1     0          0         0              -
...
```

Related commands

clear loop-protection counters

loop-protection action

loop-protection loop-detect

show mac address-table

Overview Use this command to display the MAC address-table for all configured VLANs.

Syntax

```
show mac address-table
```

Mode User Exec and Privileged Exec

Usage notes The **show mac address-table** command is only applicable to view a MAC address-table for Layer 2 switched traffic within VLANs.

Example To display the MAC address-table, use the following command:

```
awplus# show mac address-table
```

Output See the following sample output captured when there was no traffic being switched:

```
awplus#show mac address-table

VLAN port         mac              type
1    unknown      0000.cd28.0752   forward   static
ARP  -            0000.cd00.0000   forward   static
```

See the sample output captured when packets were switched and MAC addresses were learned:

```
awplus#show mac address-table

VLAN port         mac              type
1    unknown      0000.cd28.0752   forward   static
1    port1.0.2    0030.846e.9bf4   forward   dynamic
1    port1.0.3    0030.846e.bac7   forward   dynamic
ARP  -            0000.cd00.0000   forward   static
```

Note the new MAC addresses learned for port1.0.2 and port1.0.3 added as dynamic entries.

Note the first column of the output below shows VLAN IDs if multiple VLANs are configured:

```
awplus#show mac address-table

VLAN port         mac              type
1    unknown      0000.cd28.0752   forward   static
1    port1.0.2    0030.846e.bac7   forward   dynamic
2    unknown      0000.cd28.0752   forward   static
2    port1.0.3    0030.846e.9bf4   forward   dynamic
ARP  -            0000.cd00.0000   forward   static
```

Also note if manually configured static MAC addresses exist, this is shown to the right of the type column:

```
awplus(config)#mac address-table static 0000.1111.2222 for int
port1.0.3 vlan 1
awplus(config)#end
awplus#
awplus#show mac address-table

VLAN port         mac              type
1    unknown      0000.cd28.0752   forward   static
1    port1.0.2    0030.846e.bac7   forward   dynamic
1    port1.0.3    0000.1111.2222   forward   static
...
```

Related commands

clear mac address-table dynamic

clear mac address-table static

mac address-table static

show mac address-table thrash-limit

Overview Use this command to display the current thrash limit set for all interfaces on the device.

Syntax

```
show mac address-table thrash-limit
```

Mode User Exec and Privileged Exec

Example To display the current, use the following command:

```
awplus# show mac address-table thrash-limit
```

Output Figure 15-6: Example output from the **show mac address-table thrash-limit** command

```
% Thrash-limit  7 movements per second
```

Related commands mac address-table thrash-limit

show platform

Overview This command displays the settings configured by using the **platform** commands.

Syntax

```
show platform
```

Mode Privileged Exec

Usage notes This command displays the settings in the running config. For changes in some of these settings to take effect, the device must be rebooted with the new settings in the startup config.

Example To check the settings configured with **platform** commands on the device, use the following command:

```
awplus# show platform
```

Output Figure 15-7: Example output from the **show platform** command:

```
awplus#show platform
MAC vlan hashing algorithm    crc32l
L3 hashing algorithm          crc32l
Load Balancing                src-dst-ip
stop-unreg-mc-flooding        off
Vlan-stacking TPID            0x8100
Hardware Filter Size          ipv4-limited-ipv6
```

Table 16: Parameters in the output of the **show platform** command. Note that the parameters displayed depend on your device, and that not all displayed parameters can be modified on all devices.

Parameter	Description
Routing Ratio	Whether all memory is allocated to IPv4 address table entries only, or whether it is allocated evenly to both IPv4 and IPv6 addresses (set with the **platform routingratio** command).
Route Weighting	The split between multicast and unicast route entries (set with the **platform routingratio** command).
MAC vlan hashing algorithm	The MAC VLAN hash-key-generating algorithm (set with the **platform mac-vlan-hashing-algorithm** command). The default algorithm is crc32l. The algorithm may need to be changed in rare circumstances in which hash collisions occur.
L3 hashing algorithm	The L3 VLAN hash-key-generating algorithm (set with the **platform l3-vlan-hashing-algorithm** command). The default algorithm is crc32l. The algorithm may need to be changed in rare circumstances in which hash collisions occur.
Load Balancing	Which packet fields are used in the channel load balancing algorithm (set with the **platform load-balancing** command).

Table 16: Parameters in the output of the **show platform** command. Note that the parameters displayed depend on your device, and that not all displayed parameters can be modified on all devices. (cont.)

Parameter	Description
Control-plane-prioritization	Maximum traffic rate on the CPU port (set with the **platform control-plane-prioritization rate** command).
Fdb-chain-length	The length of the FDB hash chain (set with the **platform fdb-chain-length** command). FDB entries are hashed and indexed using a hash. In rare circumstances it may be useful to reduce the chain length.
L2MC overlapped group check	Whether Layer 2 multicast entries are checked before deletion (set with the **platform l2mc-overlap** command).
silicon-profile	The silicon profile setting (set with the **platform silicon-profile** command) for the switch hardware; one of: • profile 1 • profile 2 • profile 3 • None (default)
fdb-l3-hosts mode	Whether Host Mode is turned on or not. Host Mode increases the number of host entries and is available for systems containing SBx81CFC960 controller cards and SBx81XLEM line cards. See **platform silicon-profile** and **platform fdb-l3-hosts** for details.
Jumboframe support	Whether the jumbo frames setting is enabled or disabled (set with the **platform jumboframe** command).
Traffic Manager	A test setting that is disabled by default.
stop-unreg-mc-flooding	Whether the stop-unreg-mc-flooding feature is on or off (set with the **platform stop-unreg-mc-flooding** command). This feature prevents flooding of unregistered multicast packets in the occasional situations in which IGMP snooping does not prevent it.
Port Mode	Whether each port on the AT-StackQS is configured as one 40Gbps port or four 10Gbps ports, if they are operating as network ports (set with the **platform portmode interface** command).
Vlan-stacking TPID	The value of the TPID set in the Ethernet type field when a frame has a double VLAN tag (set with the **platform vlan-stacking-tpid** command).
PBR enabled	Whether policy-based routing is globally enabled or not (set with the **platform pbr-enable** command).

Table 16: Parameters in the output of the **show platform** command. Note that the parameters displayed depend on your device, and that not all displayed parameters can be modified on all devices. (cont.)

Parameter	Description
Hardware Filter Size	Whether hardware ACLs can filter on IPv6 addresses (ipv4-full-ipv6) or not (ipv4-limited-ipv6). This is set with the **platform hwfilter-size** command.
Vlan Ingress Filter Hard Drop	The Bridge Vlan Ingress Filtering drops traffic if the VID assigned to the packet does not match with the port's VLAN membership. There are two ways the traffic is dropped by the Ingress Filtering mechanism: • HARD DROP - Traffic is dropped by the Bridge Engine and not forwarded or trapped. • SOFT DROP - Traffic may be mirrored or trapped by the Bridge Engine.

show platform classifier statistics utilization brief

Overview This command displays the number of used entries available for various platform functions, and the percentage that number of entries represents of the total available.

Syntax
```
show platform classifier statistics utilization brief
```

Mode Privileged Exec

Example To display the platform classifier utilization statistics, use the following command:

```
awplus# show platform classifier statistics utilization brief
```

Output Figure 15-8: Output from **show platform classifier statistics utilization brief**

```
[Instance 0]
 Capacity:  503
  Number of Entries:
  Policy Type      Group ID   Used / Allocated
  ------------------------------------------------
  ACL              1476395010  119 /  119 (100%)
   Interface                  119
   VACL                         0
   AMFAPPS                      0
  DoS              Inactive      0 /    0 (  0%)
  VLAN Counter
   Group-Octet     Inactive      0 /    0 (  0%)
   Group-Packet    Inactive      0 /    0 (  0%)
  Flooding Nexthop Redirects Inactive      0 /    0 (  0%)
  Remote-Mirror    Inactive      0 /    0 (  0%)
  VLAN Isolate     Inactive      0 /    0 (  0%)
  QoS              Inactive      0 /    0 (  0%)

Rule Limit Reached (clear on read): 0
Total Rule Limit Reached from startup: 0
```

Output parameters Depending on your switch, you will see some of the following parameters in the output from **show platform classifier statistics utilization brief**

Parameter	Description
`IPv6 Multicast`	Reserved hardware space for use by IPv6 multicast, when the ipv6 multicast-routing command is used.
`System`	Fixed system entries. For example, resiliency links make use of system ACLs.
`MLD Snooping`	Entries to send various packets that MLD Snooping is interested in to the CPU.

Parameter	Description
DHCP Snooping	Entries used to send DHCP and ARP packets to the CPU. User-added DHCP Snooping filters under ACLs are counted under the ACL or QoS categories.
Loop Detection	Entries uses to send the special loop detection frame to the CPU.
EPSR	Entries used to send EPSR control traffic to the CPU.
CFM	Entries used by Connectivity Fault Management.
G8032	Entries used to send G.8032 control traffic to the CPU.
Global ACLs	Entries for ACLs appear here if the ACLs are applied globally instead of per switchport.
ACL	Entries for ACL filters that have been applied directly to ports using the access-group command.
VACL	Entries for VLAN-based ACLs (ACLs that are applied to VLANs instead of ports).
DOS	Entries used for Denial of Service protection.
UFO	Entries used by Upward Forwarding Only (UFO).
QoS	Entries for ACL filters and other class-map configurations, such as policers, applied through policy maps using the service input command.
RA Guard	Entries used to block IPv6 router advertisements, configured with the **ipv6 nd raguard** command.
AMFAPPS	Entries used by AMF Application Proxy. These entries enable the SES Controller to block infected ports.
Pre-Ingress	Entries used for VLAN ID Translation (and also for subnet-based and MAC-based VLAN entries on SBx81XLEM cards).
Egress	Entries used for VLAN ID Translation.
UDB	User Defined Bytes (UDB), which are a limited resource of bytes that can be used to implement additional arbitrary matching on packet bytes on some switches. The software manages the use and allocation of these bytes automatically. The output of this table is intended for use by Allied Telesis Customer Support only.

Related commands

show platform

ipv6 access-list (named IPv6 hardware ACL)

show platform port

Overview This command displays the various port registers or platform counters for specified switchports.

Syntax

```
show platform port [<port-list>] [counters]
```

Parameter	Description
<port-list>	The ports to display information about. A port-list can be: • 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).
`counters`	Show the platform counters.

Mode Privileged Exec

Examples To display port registers for port1.0.1 to port1.0.4, use the command:

```
awplus# show platform port port1.0.1-port1.0.4
```

To display platform counters for port1.0.1 to port1.0.4, use the command:

```
awplus# show platform port port1.0.1-port1.0.4 counters
```

Output Figure 15-9: Example output from the **show platform port** command

```
awplus#show platform port
Phy register value for port1.0.1 (ifindex: 5001)

BCM54220S PHY detected

00:1140  01:7949  02:600d  03:8585  04:01e1  05:0000  06:0064  07:2001
08:0000  09:0300  0a:0000  0b:0000  0c:0000  0d:4007  0e:0000  0f:3000
10:0001  11:0001  12:0000  13:1000  14:0000  15:1000  16:0000  17:0000
18:8000  19:0000  1a:0000  1b:0000  1c:0000  1d:0008  1e:0031  1f:0031
IEEE registers
00:1140  01:7949  02:600d  03:8585  04:01e1  05:0000  06:0064  07:2001
08:0000  09:0300  0a:0000  0f:300
01000X registers
00:1140  01:7949  04:01e1  05:0000
Clause 45 registers (addr:00ddrrrr d=DEVAD, r=regaddr)
00010000:0040  00010001:0002  00030001:0042  00030014:0000
007003c:0000  0007803d:0000  0007803e:0000  0007803f:0000
RDB registers (addr:value)
000:0001 001:0000 005:0820 006:c000 009:1000 00a:0000 00b:0000 00c:8000
```

```
Port configuration for lport 0x0800201a:
Phy Driver: 542XX Gigabit PHY Driver
  enabled:                1
  loopback:               0
  link:                   1
  speed:               1000  max speed:               1000
  duplex:                 1
  linkscan:               1
  autonegotiate:          1
  master:                 2
  tx pause:               0  rx pause:                   0
  untagged vlan:          1
  vlan filter:            3
  stp state:              4
  learn:                  5
  discard:                0
  jam:                    0
  max frame size:      1482
  MC Disable SA:         no
  MC Disable TTL:        no
  MC egress untag:        0
  MC egress vid:          1
  MC TTL threshold:      -1
...
```

show port-security interface

Overview Use this command to show the current port-security configuration and status.

Syntax

```
show port-security interface <port>
```

Parameter	Description
<port>	Specify the switch port to display information about, e.g. port1.0.4.

Mode Privileged Exec

Example To see the port-security status on port1.0.2, use the following command:

```
awplus# show port-security interface port1.0.2
```

Output Figure 15-10: Example output from the **show port-security interface** command

```
Port Security configuration
Security Enabled              : YES
Port Status                   : ENABLED
Violation Mode                : TRAP
Aging                         : OFF
Maximum MAC Addresses         : 3
Total MAC ddresses            : 1
Lock Status                   : UNLOCKED
Security Violation Count      : 0
Last Violation Source Address : None
```

Related commands

clear port-security intrusion

show port-security intrusion

switchport port-security

switchport port-security aging

switchport port-security maximum

switchport port-security violation

show port-security intrusion

Overview Use this command to show the intrusion list. If the port is not specified, the entire intrusion table is shown.

Syntax

```
show port-security intrusion [interface <port>]
```

Parameter	Description
`interface`	Specify a port
<port>	Specify the switch port to display information about, e.g. port1.0.4.

Mode Privileged Exec

Example To see the intrusion list on port1.0.2, use the following command:

```
awplus# show port-security intrusion interface port1.0.2
```

Output Figure 15-11: Example output from the **show port-security intrusion** command for port1.0.2

```
Port Security Intrusion List
Interface: port1.0.2 -3 intrusion(s) detected
11-22-33-44-55-04 11-22-33-44-55-06 11-22-33-44-55-08
```

Related commands

clear port-security intrusion

show port-security interface

switchport port-security

switchport port-security aging

switchport port-security maximum

switchport port-security violation

show storm-control

Overview Use this command to display storm-control information for all interfaces or a particular interface.

Syntax

```
show storm-control [<port>]
```

Parameter	Description
<port>	The port to display information about. The port may be: • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2)

Mode User Exec and Privileged Exec

Example To display storm-control information for port1.0.2, use the following command:

```
awplus# show storm-control port1.0.2
```

Output Figure 15-12: Example output from the **show storm-control** command for port1.0.2

```
Port       BcastLevel  McastLevel  DlfLevel
port1.0.2      40. 0%     100. 0%   100. 0%
```

Related commands storm-control level

speed

Overview This command changes the speed of the specified port. You can optionally specify the speed or speeds that get autonegotiated, so autonegotiation is only attempted at the specified speeds.

To see the currently-negotiated speed for ports whose links are up, use the show interface command. To see the configured speed (when different from the default), use the show running-config command.

Syntax

```
speed {10|100|1000}
speed auto [10] [100] [1000]
```

The following table shows the speed options for each type of port.

Port type	Speed Options (units are Mbps)

RJ-45 copper ports	`auto` (default)
	`10`
	`100`
	`1000`

100 Mbps fiber SFPs	`100`
1000 Mbps fiber SFPs	`auto` (default) `1000`

Mode Interface Configuration

Default By default, ports autonegotiate speed (except for 100Base-FX ports which do not support auto-negotiation, so default to 100 Mbps).

Usage notes We recommend having autonegotiation enabled for link speeds of 1000 Mbps and above. For example, to apply a fixed speed of 1000 Mbps use the command **speed auto 1000**.

If multiple speeds are specified after the auto option to autonegotiate speeds, then the device only attempts autonegotiation at those specified speeds.

Switch ports in a static or dynamic (LACP) channel group must have the same port speed and be in full duplex mode. Once switch ports have been aggregated into a channel group, you can set the speed of all the switch ports in the channel group by applying this command to the channel group.

Examples To set a port to auto-negotiate its speed at 1000 Mbps only, which will fix this port speed to 1000 Mbps, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed auto 1000
```

To return the port to auto-negotiating its speed, enter the following commands:

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

Related commands

duplex

ecofriendly lpi

polarity

show interface

speed (asyn)

storm-control level

Overview Use this command to specify the speed limiting level for broadcast, multicast, or dlf (destination lookup failure) traffic for the port. Storm-control limits the selected traffic type to the specified percentage of the maximum port speed.

Use the **no** variant of this command to disable storm-control for broadcast, multicast or dlf traffic.

Syntax

```
storm-control {broadcast|multicast|dlf} level <level>
no storm-control {broadcast|multicast|dlf} level
```

Parameter	Description
<level>	<0-100> Specifies the percentage of the maximum port speed allowed for broadcast, multicast or destination lookup failure traffic.
broadcast	Applies the storm-control to broadcast frames.
multicast	Applies the storm-control to multicast frames.
dlf	Applies the storm-control to destination lookup failure traffic.

Default Disabled

Mode Interface Configuration

Usage notes Flooding techniques are used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

More than one limit type can be set at a time. For example, you can configure both broadcast and multicast levels on the same port, at the same time.

Example To limit broadcast traffic on port1.0.2 to 30% of the maximum port speed, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# storm-control broadcast level 30
```

Related commands show storm-control

Command changes Version 5.4.9-1.3: Multiple limit types available on x530 series

Version 5.5.0-2.1: Multiple limit types available on x220 and GS980M series

switchport port-security

Overview Use this command to enable the port-security feature. This feature is also known as the port-based learn limit. It allows you to set the maximum number of MAC addresses that each port can learn (using the switchport port-security maximum command).

Use the **no** variant of this command to disable the port-security feature.

Syntax

```
switchport port-security
no switchport port-security
```

Mode Interface Configuration for a switchport.

Usage notes After using this command to turn on port-security, use the following commands to configure it:

- switchport port-security maximum to set the number of MAC addresses that can be learned
- switchport port-security aging (optional) to choose whether to limit it to specific devices, or to allow any devices up to the limit
- switchport port-security violation (optional) to change the action the switch takes if the limit is violated.

If the switch sees a new MAC address on a port that has port-security enabled, and the MAC address is statically configured for another port, this triggers a violation. The switch will ignore the maximum learn limit and will treat that MAC address as an intruder.

Examples To enable the port-security feature on port1.0.2 and set it to learn 1 MAC address, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport port-security
awplus(config-if)# switchport port-security maximum 1
```

To disable the port-security feature on port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport port-security
```

Related commands

clear port-security intrusion

show port-security interface

show port-security intrusion

switchport port-security aging

switchport port-security maximum

switchport port-security violation

Command changes

Version 5.5.1-0.1: port-security on LAGs added for SBx81CFC960, SBx908 GEN2, x950, x930, x550, x530, x530L, x320, x230, x230L and x220 Series switches

switchport port-security aging

Overview Use this command to set MAC addresses that have been learned by port security to age out.

Use the **no** variant of this command to set the MAC addresses to not age out.

Syntax

```
switchport port-security aging
no switchport port-security aging
```

Default Disabled (MAC addresses do not age out)

Mode Interface Configuration for a switchport.

Usage notes Use this command to change from static to dynamic operation.

Static operation

Any MAC address learned will be statically installed into the MAC Address table and will not age out. The addresses are also added to the device's running configuration. Each entry then counts towards the maximum allowed addresses, regardless of whether the device is still connected.

Use this if you want to allow only specific devices to access the port. For example, this can prevent a person from plugging an unauthorized laptop into your corporate LAN.

This is the default mode.

Dynamic operation

Any MAC addresses learned will be dynamically installed into the MAC Address table. Unlike the static operation, no MAC addresses are added to the device's running configuration. If a device is disconnected, the Maximum MAC addresses allowed decreases by 1 (once the dynamic entry times out in the MAC Address table).

Use this if you want to allow only a limited number of devices to access the port, but you are not concerned about which specific devices have access. For example, this can prevent a person from plugging a switch into a port and creating an unauthorized internet cafe.

Examples To choose dynamic mode by setting port1.0.2 so that the MAC addresses that have been learned by port security age out, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport port-security aging
```

To return to static mode by stopping the MAC addresses that have been learned by port security from aging out on port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport port-security aging
```

Related commands

clear port-security intrusion

show port-security interface

show port-security intrusion

switchport port-security

switchport port-security maximum

switchport port-security violation

Command changes

Version 5.5.1-0.1: port-security on LAGs added for SBx81CFC960, SBx908 GEN2, x950, x930, x550, x530, x530L, x320, x230, x230L and x220 Series switches

switchport port-security maximum

Overview Use this command to set the maximum number of MAC addresses that each port can learn when port-security is enabled on that port.

Use the **no** variant of this command to unset the maximum number of MAC addresses that can be learned. This is same as setting the maximum number to 0. This command also resets the intrusion list table.

Syntax

```
switchport port-security maximum <0-256>
no switchport port-security maximum
```

Parameter	Description
`maximum <0-256>`	Specify the maximum number of addresses to learn.

Mode Interface Configuration for a switchport.

Usage notes Before using this command, turn on port-security with the switchport port-security command.

After using this command to specify the limit, you can use the following commands for further configuration:

- switchport port-security aging (optional) to choose whether to limit it to specific devices, or to allow any devices up to the limit
- switchport port-security violation (optional) to change the action the switch takes if the limit is violated.

If the switch sees a new MAC address on a port that has port-security enabled, and the MAC address is statically configured for another port, this triggers a violation. The switch will ignore the maximum learn limit and will treat that MAC address as an intruder.

Examples To learn 3 MAC addresses on port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport port-security
awplus(config-if)# switchport port-security maximum 3
```

To remove the MAC learning limit on port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport port-security maximum
```

Related commands

clear port-security intrusion

show port-security interface

show port-security intrusion

switchport port-security

switchport port-security aging

switchport port-security violation

Command changes

Version 5.5.1-0.1: port-security on LAGs added for SBx81CFC960, SBx908 GEN2, x950, x930, x550, x530, x530L, x320, x230, x230L and x220 Series switches

switchport port-security violation

Overview Use this command to set the action taken on a switch port when the port exceeds the port-security learning limits.

The action can be **shutdown**, **restrict** or **protect**:

- **shutdown**: the physical link will be disabled and 'shutdown' will be shown in the configuration file.
- **restrict**: the packet from the unauthorized MAC will be discarded and an SNMP trap will be generated to alert management.
- **protect**: the packet will simply be discarded silently.

Use the **no** variant of this command to set the violation action to the default action of **protect**.

Syntax

```
switchport port-security violation {shutdown|restrict|protect}
no switchport port-security violation
```

Parameter	Description
`shutdown`	Disable the port.
`restrict`	Discard and alert the network administrator.
`protect`	Discard the packet.

Mode Interface Configuration for a switchport.

Default Protect

Usage notes When modes restrict or shutdown are used, the administrator can also be alerted via an SNMP trap. To configure this, add the following command to the SNMP configuration:

```
awplus(config)# snmp-server enable trap nsm
```

Examples To set the action to be shutdown on port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport port-security violation shutdown
```

To set the port-security action to the default (protect) on port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport port-security violation
```

Related commands

clear port-security intrusion

show port-security interface

show port-security intrusion

switchport port-security

switchport port-security aging

switchport port-security maximum

Command changes

Version 5.5.1-0.1: port-security on LAGs added for SBx81CFC960, SBx908 GEN2, x950, x930, x550, x530, x530L, x320, x230, x230L and x220 Series switches

thrash-limiting

Overview Use this command to configure the thrash limit action that will be applied to a port on the device when a thrashing condition is detected. The thrash-limiting timeout specifies the time, in seconds, for which the action is employed.

Use the **no** variant of this command to return the action or timeout to its default setting.

Syntax

```
thrash-limiting {[action
{learn-disable|link-down|port-disable|vlan-disable|none}]
[timeout <0-86400>]}
```

```
no thrash-limiting {action|timeout}
```

Parameter	Description
`action`	The action taken when MAC thrashing is detected.
`learn-disable`	Disable MAC address learning
`link-down`	Block all traffic on an interface - link down
`port-disable`	Block all traffic on an interface - link remains up
`vlan-disable`	Block all traffic on a VLAN if the switch detects thrashing for that VLAN on the selected port. Note that setting this parameter will also enable ingress filtering.
`none`	No thrash action
`timeout`	Set the duration for the thrash action
`<0-86400>`	The duration of the applied thrash action in seconds. The default is 1 seconds.

Default The default action is learn-disable and the default timeout is 1 second.

Mode Interface Configuration

Usage Thrash-limiting actions are initiated when MAC addresses are added and removed from a port's MAC table faster than a given rate. The rate is 10 MAC address changes per second by default. You can change it with the mac address-table thrash-limit command.

See the "Thrash Limiting" section in the Switching Feature Overview and Configuration Guide for more information.

Examples To set the action to learn disable for port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# thrash-limiting action learn-disable
```

To block all traffic on a VLAN on port1.0.1 if the switch detects thrashing for that VLAN on that port, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# thrash-limiting action vlan-disable
```

To set the thrash limiting action to its default on port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no thrash-limiting action
```

To set the thrash limiting timeout to 5 seconds on port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# thrash-limiting timeout 5
```

To set the thrash limiting timeout value to its default on port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no thrash-limiting timeout
```

Related commands

mac address-table thrash-limit

show interface

undebug loopprot

Overview This command applies the functionality of the no debug loopprot command.

undebug platform packet

Overview This command applies the functionality of the no debug platform packet command.

16 VLAN Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure VLANs. For more information see the VLAN Feature Overview and Configuration Guide.

Command List

- "debug private-vlan ufo" on page 613
- "platform vlan-stacking-tpid" on page 614
- "port-vlan-forwarding-priority" on page 615
- "private-vlan" on page 618
- "private-vlan association" on page 620
- "private-vlan ufo trap" on page 621
- "show debugging private-vlan" on page 622
- "show interface switchport vlan translation" on page 623
- "show port-vlan-forwarding-priority" on page 625
- "show vlan" on page 626
- "show vlan access-map" on page 627
- "show vlan classifier group" on page 628
- "show vlan classifier group interface" on page 629
- "show vlan classifier interface group" on page 630
- "show vlan classifier rule" on page 631
- "show vlan filter" on page 632
- "show vlan private-vlan" on page 633
- "show vlan private-vlan ufo" on page 634
- "switchport access vlan" on page 635

- "switchport enable vlan" on page 636
- "switchport mode access" on page 637
- "switchport mode private-vlan" on page 638
- "switchport mode private-vlan trunk promiscuous" on page 639
- "switchport mode private-vlan trunk secondary" on page 641
- "switchport mode private-vlan ufo" on page 643
- "switchport mode trunk" on page 645
- "switchport private-vlan host-association" on page 646
- "switchport private-vlan mapping" on page 647
- "switchport trunk allowed vlan" on page 648
- "switchport trunk native vlan" on page 651
- "switchport vlan translation" on page 652
- "switchport vlan translation default drop" on page 654
- "switchport vlan-stacking (double-tagging)" on page 655
- "switchport voice dscp" on page 656
- "switchport voice vlan" on page 657
- "switchport voice vlan priority" on page 659
- "vlan" on page 660
- "vlan access-map" on page 662
- "vlan classifier activate" on page 663
- "vlan classifier group" on page 664
- "vlan classifier rule ipv4" on page 665
- "vlan classifier rule proto" on page 666
- "vlan database" on page 669
- "vlan filter" on page 670

debug private-vlan ufo

Overview Use this command to enable private-vlan Upward Forwarding Only (UFO) debugging.

Use the **no** variant of this command to disable private-vlan UFO debugging.

Syntax

```
debug private-vlan ufo
no debug private-vlan ufo
```

Mode Privileged Exec

Usage notes Use this command to enable or disable private-vlan ufo debugging.

Example To enable private-vlan UFO debugging, use the commands:

```
awplus# configure terminal
awplus(config)# debug private-vlan ufo
```

Related commands

show debugging private-vlan

private-vlan ufo trap

switchport mode private-vlan ufo

Command changes

Version 5.4.7-2.1: command added

Version 5.4.8-2.1: added to SBx8100 Series products

Version 5.4.9-0.1: added to x530 Series products

platform vlan-stacking-tpid

Overview This command specifies the Tag Protocol Identifier (TPID) value that applies to all frames that are carrying double tagged VLANs. All such VLANs must use the same TPID value. (This feature can be referred to as nested VLANs, VLAN stacking, Q-in-Q, or VLAN double-tagging.)

Use the **no** variant of this command to revert to the default TPID value (0x8100).

NOTE: *Because the additional tag increases the frame size beyond 1522 bytes, you must increase the MRU size to activate VLAN-stacking. Go into interface mode for the appropriate ports and use the mru command.*

Syntax

```
platform vlan-stacking-tpid <tpid>
no platform vlan-stacking-tpid
```

Parameter	Description
<tpid>	The Ethernet type of the tagged packet, as a two byte hexadecimal number.

Default The default TPID value is 0x8100.

Mode Global Configuration

Examples To set the VLAN stacking TPID value to 0x9100, use the following commands:

```
awplus# configure terminal
awplus(config)# platform vlan-stacking-tpid 9100
```

To reset the VLAN stacking TPID value to the default (0x8100), use the following commands:

```
awplus# configure terminal
awplus(config)# no platform vlan-stacking-tpid
```

Related commands

switchport vlan-stacking (double-tagging)

show platform

show running-config

port-vlan-forwarding-priority

Overview Use this command to specify which protocol has the highest priority for controlling transitions from blocking to forwarding traffic, when more than one of EPSR, Loop Protection, and MAC thrashing protection are used on the switch.

These protocols use the same mechanism to block or forward traffic. This command specifies either EPSR or Loop Protection as the highest priority protocol. Setting the priority stops contention between protocols.

For more information, see the Usage section below.

CAUTION: *The **loop-protection** and **none** parameter options must not be set on an EPSR master node. Use the **epsr** parameter option on an EPSR master node instead. Setting this command incorrectly on an EPSR master node could cause unexpected broadcast storms.*

Use the **no** variant of this command to restore the default highest priority protocol back to the default of EPSR.

For more information about EPSR, see the EPSR Feature Overview and Configuration_Guide.

Syntax

```
port-vlan-forwarding-priority {epsr|loop-protection|none}
no port-vlan-forwarding-priority
```

Parameter	Description
`epsr`	Sets EPSR as the highest priority protocol. Use this parameter on an EPSR master node to avoid unexpected broadcast storms.
`loop-protection`	Sets Loop Protection as the highest priority protocol. Note that this option must not be set on an EPSR master node. Use the **epsr** parameter option on an EPSR master node to avoid unexpected broadcast storms.
`none`	Sets the protocols to have equal priority. This allows protocols to override each other to set a port to forwarding for a VLAN. Note that this option must not be set on a EPSR master node. Use the **epsr** parameter option on an EPSR master node to avoid unexpected broadcast storms.

Default By default, the highest priority protocol is EPSR

Mode Global Configuration

Usage notes Usually, you only need to configure one of EPSR, Loop Protection and MAC Thrashing protection on a switch, because they perform similar functions—each prevents network loops by blocking a selected port for each (loop-containing) VLAN.

However, if more than one of these three features is configured on a switch, you can use this command to prioritize either EPSR or Loop Protection when their

effects on a port would conflict and override each other. Without this command, each protocol could set a port to forwarding for a VLAN, sometimes overriding the previous setting by another protocol to block the port. This could sometimes lead to unexpected broadcast storms.

This command means that, when a protocol is set to have the highest priority over a data VLAN on a port, it will not allow other protocols to put that port-vlan into a forwarding state if the highest priority protocol blocked it.

The priority mechanism is only used for blocking-to-forwarding transitions; protocols remain independent on the forwarding-to-blocking transitions.

For example, consider an EPSR master node in a two-node ESPR ring with the following settings:

- The EPSR master node primary port is configured to switchport interface port1.0.1
- The EPSR master node secondary port is configured to switchport interface port1.0.2
- The EPSR master node control VLAN is configured to VLAN interface vlan10
- The EPSR master node has a first data VLAN configured to VLAN interface vlan20
- The EPSR master node has a second data VLAN configured to VLAN interface vlan30.

Initially, the EPSR ring is complete, with port1.0.2 blocking data VLANs vlan20 and vlan30 and some broadcast traffic flowing through. If the user removes vlan30 from EPSR, a storm is created on vlan30. MAC thrashing protection detects it and blocks vlan30.

Then after the storm has stopped, MAC thrashing protection sets it to forwarding again and it keeps oscillating between forwarding and blocking. In the meantime, the user adds back vlan30 to EPSR as a data VLAN and EPSR blocks it on port1.0.2.

If the priority is set to none (**port-vlan-forwarding-priority none**), MAC thrashing protection notices that the storm has stopped again and decides to put vlan30 on port1.0.2 into forwarding state. This overrides what EPSR requires for this port-VLAN and creates a storm.

If the priority is set to EPSR or default (**port-vlan-forwarding-priority epsr**), MAC thrashing protection notices that the storm has stopped again and attempts to put vlan30 on port1.0.2 into forwarding state. The higher priority protocol (EPSR) is blocking the VLAN on this port, so it stays blocking and no storm occurs.

Example To prioritize EPSR over Loop Protection or MAC Thrashing protection settings, so that Loop Protection or MAC Thrashing protection cannot set a port to the forwarding state for a VLAN if EPSR has set it to the blocking state, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority epsr
```

To prioritize Loop Protection over EPSR or MAC Thrashing protection settings, so that EPSR or MAC Thrashing protection cannot set a port to the forwarding state for a VLAN if Loop Protection has set it to the blocking state, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority loop-protection
```

To set EPSR, Loop Protection, and MAC Thrashing protection protocols to have equal priority for port forwarding and blocking, which allows the protocols to override each other to set a port to the forwarding or blocking states, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority none
```

To restore the default highest priority protocol back to the default of EPSR, use the commands:

```
awplus# configure terminal
awplus(config)# no port-vlan-forwarding-priority
```

Related commands show port-vlan-forwarding-priority

private-vlan

Overview Use this command to a create a private VLAN. Private VLANs can be either primary or secondary. Secondary VLANs can be either community or isolated.

Alternatively, private VLANs can be UFO (Upstream Forwarding Only). Private VLAN port members are either 'downstream' or 'upstream'. Once a private VLAN is configured as UFO, its port members by default are downstream.

Use the **no** variant of this command to remove the specified private VLAN.

For more information, see the VLAN Feature Overview and Configuration Guide.

Syntax

```
private-vlan <vlan-id> {community|isolated|primary|ufo}
no private-vlan <vlan-id> {community|isolated|primary|ufo}
```

Parameter	Description
<vlan-id>	VLAN ID in the range <2-4094> for the VLAN which is to be made a private VLAN.
community	Community VLAN.
isolated	Isolated VLAN.
primary	Primary VLAN.
ufo	Upstream Forwarding Only (UFO) VLAN.

Mode VLAN Configuration

Examples To configure a set of private VLANs, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2 name vlan2 state enable
awplus(config-vlan)# vlan 3 name vlan3 state enable
awplus(config-vlan)# vlan 4 name vlan4 state enable
awplus(config-vlan)# private-vlan 2 primary
awplus(config-vlan)# private-vlan 3 isolated
awplus(config-vlan)# private-vlan 4 community
```

To remove a set of private VLANs, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no private-vlan 2 primary
awplus(config-vlan)# no private-vlan 3 isolated
awplus(config-vlan)# no private-vlan 4 community
```

To configure a private VLAN for Upward Forwarding Only (UFO), use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 512 name vlan512 state enable
awplus(config-vlan)# private-vlan 512 ufo
```

Related commands

show vlan private-vlan

Command changes

Version 5.4.7-2.1: **ufo** parameter added

Version 5.4.8-2.1: **ufo** parameter added to SBx8100 Series products

Version 5.4.9-0.1: **ufo** parameter added to x530 Series products

private-vlan association

Overview Use this command to associate a secondary VLAN to a primary VLAN. Only one isolated VLAN can be associated to a primary VLAN. Multiple community VLANs can be associated to a primary VLAN.

Use the **no** variant of this command to remove association of all the secondary VLANs to a primary VLAN.

For more information, see the VLAN_Feature Overview and Configuration Guide.

Syntax

```
private-vlan <primary-vlan-id> association {add
<secondary-vlan-id>|remove <secondary-vlan-id>}
```

```
no private-vlan <primary-vlan-id> association
```

Parameter	Description
<primary-vlan-id>	VLAN ID of the primary VLAN.
<secondary-vlan-id>	VLAN ID of the secondary VLAN (either isolated or community).

Mode VLAN Configuration

Examples The following commands associate primary VLAN 2 with secondary VLAN 3:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 2 association add 3
```

The following commands remove the association of primary VLAN 2 with secondary VLAN 3:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 2 association remove 3
```

The following commands remove all secondary VLAN associations of primary VLAN 2:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no private-vlan 2 association
```

private-vlan ufo trap

Overview Use this command to enable the sending of SNMP traps for private VLAN UFO.

Use the **no** variant of this command to disable the sending of SNMP traps for private VLAN UFO.

Syntax

```
private-vlan ufo trap
no private-vlan ufo trap
```

Parameter	Description
ufo	Specifies private-vlan for those VLANs in UFO mode.
trap	Enables or disables SNMP trap sending for private-vlan UFO.

Default Enabled.

Mode Global Configuration

Usage notes This command enables SNMP traps for private-vlan UFO. If enabled, traps will be sent when any UFO VLAN becomes "isolated", which occurs when traffic can not be forwarded at Layer 2 because there is no upstream port for the UFO VLAN, and Layer3 forwarding has not been configured for the VLAN.

Example To configure a private-vlan UFO trap use the commands:

```
awplus# configure terminal
awplus(config)# private-vlan ufo trap
```

Related commands private-vlan

snmp-server enable trap

Command changes Version 5.4.7-2.1: command added

Version 5.4.8-2.1: added to SBx8100 Series products

Version 5.4.9-0.1: added to x530 Series products

show debugging private-vlan

Overview Use this command to show whether debugging for a private-vlan, namely UFO, is enabled.

Syntax

```
show debugging private-vlan
```

Mode Privileged Exec

Example To show if debugging is enabled for private-vlan UFO, use the command:

```
awplus# show debugging private-vlan
```

Output Figure 16-1: Example output from **show debugging private-vlan**

```
awplus#show debugging private-vlan

Private-VLAN debugging status:
UFO debugging is off
```

Related commands debug private-vlan ufo

Command changes Version 5.4.7-2.1: command added.

Version 5.4.8-2.1: added to SBx8100 Series products

Version 5.4.9-0.1: added to x530 Series products

show interface switchport vlan translation

Overview Use this command to display VLAN translation information for some or all interfaces.

Syntax

```
show interface switchport vlan translation [interface <int>]
```

Parameter	Description
`interface <int>`	The interface to display information about. An interface can be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2).

Mode User Exec and Privileged Exec

Example To display VLAN translation information for port1.0.1, use the command:

```
awplus# show interface switchport vlan translation interface
port1.0.1
```

Output Figure 16-2: Example output from **show interface switchport vlan translation interface port1.0.1**

```
awplus#show interface switchport vlan translation interface
port1.0.1

VLAN on Wire            VLAN                Outer Vlan
================        ================    ================
200                     100                 300
default                 accept
```

Output Figure 16-3: Example output from **show interface switchport vlan translation**

```
awplus#show interface switchport vlan translation

Interface: port1.0.1
VLAN on Wire            VLAN                Outer Vlan
================        ================    ================
200                     100                 300
default                 accept

Interface: port1.0.2
VLAN on Wire            VLAN                Outer Vlan
================        ================    ================
69                      1
default                 accept
```

Table 16-1: Parameters in the output from **show interface switchport vlan translation**

Parameter	Description
Interface	The interface on which VLAN-IDs will be translated.
VLAN on Wire	VLAN-ID of the packet as it will be seen on the wire.
VLAN	VLAN-ID of the VLAN as it was assigned when the VLAN was created.
Outer Vlan	VLAN-ID of the outer-tag-VLAN added by VLAN double-tagging.
default	The action taken on inbound tagged packets that do not match a VLAN translation entry; either **drop** or **accept**.

Related commands

switchport vlan translation

switchport vlan translation default drop

Command changes

Version 5.4.8-0.2: added to SBx908 GEN2, x930 Series products

Version 5.4.8-1.1: added to SBx8100 Series products

Version 5.4.9-0.1: added to x530 Series products

show port-vlan-forwarding-priority

Overview Use this command to display the highest priority protocol that controls port-vlan forwarding or blocking traffic. This command displays whether EPSR or Loop Protection is set as the highest priority for determining whether a port forwards a VLAN, as set by the port-vlan-forwarding-priority command.

For more information about EPSR, see the EPSR Feature Overview and Configuration_Guide.

Syntax

```
show port-vlan-forwarding-priority
```

Mode Privileged Exec

Example To display the highest priority protocol, use the command:

```
awplus# show port-vlan-forwarding-priority
```

Output Figure 16-4: Example output from the **show port-vlan-forwarding-priority** command

```
Port-vlan Forwarding Priority: EPSR
```

Related commands port-vlan-forwarding-priority

show vlan

Overview Use this command to display information about a particular VLAN by specifying its VLAN ID. Selecting **all** will display information for all the VLANs configured.

Syntax

```
show vlan
{all|brief|dynamic|static|auto|static-ports|<1-4094>}
```

Parameter	Description
<1-4094>	Display information about the VLAN specified by the VLAN ID.
`all`	Display information about all VLANs on the device.
`brief`	Display information about all VLANs on the device.
`dynamic`	Display information about all VLANs learned dynamically.
`static`	Display information about all statically configured VLANs.
`auto`	Display information about all auto-configured VLANs.
`static-ports`	Display static egress/forbidden ports.

Mode User Exec and Privileged Exec

Example To display information about VLAN 2, use the command:

```
awplus# show vlan 2
```

Output Figure 16-5: Example output from the **show vlan** command

```
VLAN ID  Name            Type    State   Member ports
                                         (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ====================================
2       VLAN0002         STATIC  ACTIVE  port1.0.3(u) port1.0.4(u) port1.0.5(u)
                                         port1.0.6(u)
...
```

Related commands vlan

Command changes Version 5.5.0-1.3: Support for up to 5 VLANs added to AR1050V

show vlan access-map

Overview Use this command to display information about the configured VLAN access-maps. VLAN access-maps contain a series of ACLs and enable you to filter traffic ingressing specified VLANs.

Syntax

```
show vlan access-map [<name>]
```

Parameter	Description
<name>	The name of the access-map to display.

Mode User Exec/Privileged Exec

Example To display the ACLs in all access-maps, use the command:

```
awplus# show vlan access-map
```

Output Figure 16-6: Example output from **show vlan access-map**

```
awplus#show vlan access-map

Vlan access map : deny_all
Hardware MAC access list 4000
   10 deny any any

Vlan access map : ip_range
Hardware IP access list 3000
   10 deny ip 192.168.1.1/24 any
```

Related commands vlan access-map

Command changes Version 5.4.6-2.1: command added

show vlan classifier group

Overview Use this command to display information about all configured VLAN classifier groups or a specific group.

Syntax

```
show vlan classifier group [<1-16>]
```

Parameter	Description
<1-16>	VLAN classifier group identifier

Mode User Exec and Privileged Exec

Usage If a group ID is not specified, all configured VLAN classifier groups are shown. If a group ID is specified, a specific configured VLAN classifier group is shown.

Example To display information about VLAN classifier group 1, enter the command:

```
awplus# show vlan classifier group 1
```

Related commands vlan classifier group

show vlan classifier group interface

Overview Use this command to display information about a single switch port interface for all configured VLAN classifier groups.

Syntax

```
show vlan classifier group interface <switch-port>
```

Parameter	Description
<switch-port>	Specify the switch port interface classifier group identifier

Mode User Exec and Privileged Exec

Usage notes All configured VLAN classifier groups are shown for a single interface.

Example To display VLAN classifier group information for switch port interface port1.0.2, enter the command:

```
awplus# show vlan classifier group interface port1.0.2
```

Output Figure 16-7: Example output from the **show vlan classifier group interface port1.0.1** command:

```
vlan classifier group 1 interface port1.0.1
```

Related commands

vlan classifier group

show vlan classifier interface group

show vlan classifier interface group

Overview Use this command to display information about all interfaces configured for a VLAN group or all the groups.

Syntax

```
show vlan classifier interface group [<1-16>]
```

Parameter	Description
<1-16>	VLAN classifier interface group identifier

Mode User Exec and Privileged Exec

Usage notes If a group ID is not specified, all interfaces configured for all VLAN classifier groups are shown. If a group ID is specified, the interfaces configured for this VLAN classifier group are shown.

Example To display information about all interfaces configured for all VLAN groups, enter the command:

```
awplus# show vlan classifier interface group
```

To display information about all interfaces configured for VLAN group 1, enter the command:

```
awplus# show vlan classifier interface group 1
```

Output Figure 16-8: Example output from the **show vlan classifier interface group** command

```
vlan classifier group 1 interface port1.0.1
vlan classifier group 1 interface port1.0.2
vlan classifier group 2 interface port1.0.3
vlan classifier group 2 interface port1.0.4
```

Figure 16-9: Example output from the **show vlan classifier interface group** 1 command

```
vlan classifier group 1 interface port1.0.1
vlan classifier group 1 interface port1.0.2
```

Related commands vlan classifier group

show vlan classifier group interface

show vlan classifier rule

Overview Use this command to display information about all configured VLAN classifier rules or a specific rule.

Syntax

```
show vlan classifier rule [<1-256>]
```

Parameter	Description
<1-256>	VLAN classifier rule identifier

Mode User Exec and Privileged Exec

Usage If a rule ID is not specified, all configured VLAN classifier rules are shown. If a rule ID is specified, a specific configured VLAN classifier rule is shown.

Example To display information about VLAN classifier rule 1, enter the command:

```
awplus# show vlan classifier rule 1
```

Output Figure 16-10: Example output from the **show vlan classifier rule**1 command

```
vlan classifier group 1 add rule 1
```

Related commands

vlan classifier activate

vlan classifier rule ipv4

vlan classifier rule proto

show vlan filter

Overview Use this command to display information about the configured VLAN filters. VLAN filters apply access-maps (and therefore ACLs) to VLANs. This enables you to filter traffic ingressing specified VLANs.

Syntax

```
show vlan filter [<access-map-name>]
```

Parameter	Description
<access-map-name>	The name of an access-map. The command output displays only the filters that use that access-map.

Mode User Exec/Privileged Exec

Example To display information about the filter that uses the access-map named "deny_all", use the command:

```
awplus# show vlan filter deny_all
```

Output Figure 16-11: Example output from **show vlan filter**

```
awplus#show vlan filter deny_all
Vlan filter : deny_all
    direction : ingress
    vlan list : 48-49
    access map : deny_all
Hardware MAC access list 4000
   10 deny any any
```

Related commands vlan access-map

vlan filter

Command changes Version 5.4.6-2.1: command added

show vlan private-vlan

Overview Use this command to display the private VLAN configuration and associations.

Syntax

```
show vlan private-vlan
```

Mode User Exec and Privileged Exec

Example To display the private VLAN configuration and associations, enter the command:

```
awplus# show vlan private-vlan
```

Output Figure 16-12: Example output from the **show vlan private-vlan** command

```
awplus#show vlan private-vlan
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------       ---------        ----------     ----------
       2               3          isolated
       2               4         community
                       8          isolated
```

Related commands

private-vlan

private-vlan association

show vlan private-vlan ufo

Overview Use this command to show the configuration status of a private VLAN UFO-based VLAN(s) and member interfaces.

Syntax

```
show vlan private-vlan ufo {all|<vlan-id>}
```

Parameter	Description
<vlan-id>	A specific VLAN. This must have been configured previously as a private-vlan UFO.
`all`	All VLANs that have been configured previously as private-vlan UFO.

Mode User Exec/Privileged Exec.

Usage notes Private VLANs can be UFO (Upstream Forwarding Only). Private VLAN port members are either "downstream" or "upstream" which are controlled by a protocol or by static configuration.

Example To show all the private-vlan UFO interfaces, use the command:

```
awplus# show vlan private-vlan ufo all
```

Output Figure 16-13: Example output from **show vlan private-vlan ufo all**

```
awplus#show vlan private-vlan ufo all
VLAN  INTERFACES CONFIGURED         TYPE             PROTOCOL MISC
-------------------------------------------------------------------------------
100   port1.0.1  primary-upstream   upstream         UFO      -
100   port1.0.2  secondary-upstream downstream       UFO      -
100   port1.0.3  -                  downstream       Static   -
200   port1.0.4  epsr               downstream       EPSR     -
200   sa1        epsr               upstream         EPSR     0030.846e.bac7
200   port1.0.5  -                  downstream       Static   -
300   port1.0.6  -                  downstream-fault Static   -
300   port1.0.7  -                  downstream-fault Static   -
300   port1.0.8  -                  downstream-fault Static   -
400   Port1.0.9  stp                upstream         STP      0030.846e.9bf4
400   Port1.0.10 stp                downstream       STP      -
400   Port1.0.11                    downstream       Static   -
```

Command changes Version 5.4.7-2.1: command added

Version 5.4.8-2.1: added to SBx8100 Series products

Version 5.4.9-0.1: added to x530 Series products

switchport access vlan

Overview Use this command to change the port-based VLAN of the current port.

Use the **no** variant of this command to change the port-based VLAN of this port to the default VLAN, VLAN 1.

Syntax

```
switchport access vlan <vlan-id>
no switchport access vlan
```

Parameter	Description
<vlan-id>	<1-4094> The port-based VLAN ID for the port.

Default VLAN 1

Mode Interface Configuration

Usage notes Any untagged frame received on this port will be associated with the specified VLAN.

Examples To change the port-based VLAN to VLAN 3 for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport access vlan 3
```

To reset the port-based VLAN to the default VLAN 1 for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport access vlan
```

Related commands show interface switchport

show vlan

Command changes Version 5.5.0-1.3: Support for up to 5 VLANs added to AR1050V

switchport enable vlan

Overview This command enables the VLAN on the port manually once disabled by certain actions, such as QSP (QoS Storm Protection) or EPSR (Ethernet Protection Switching Ring). Note that if the VID is not given, all disabled VLANs are re-enabled.

Syntax

```
switchport enable vlan [<1-4094>]
```

Parameter	Description
`vlan`	Re-enables the VLAN on the port.
<1-4094>	VLAN ID.

Mode Interface Configuration

Example To re-enable port1.0.2 from VLAN 1:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport enable vlan 1
```

Related commands show mls qos interface storm-status

storm-window

switchport mode access

Overview Use this command to set the switching characteristics of the port to access mode. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Syntax

```
switchport mode access [ingress-filter {enable|disable}]
```

Parameter	Description
`ingress-filter`	Set the ingress filtering for the received frames.
`enable`	Turn on ingress filtering for received frames. This is the default.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default By default, ports are in access mode with ingress filtering on.

Usage notes Use access mode to send untagged frames only.

Mode Interface Configuration

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access ingress-filter enable
```

Related Commands show interface switchport

Command changes Version 5.5.0-1.3: Support for up to 5 VLANs added to AR1050V

switchport mode private-vlan

Overview Use this command to make a Layer 2 port a private VLAN host port or a promiscuous port.

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

Syntax

```
switchport mode private-vlan {host|promiscuous}
no switchport mode private-vlan {host|promiscuous}
```

Parameter	Description
`host`	This port type can communicate with all other host ports assigned to the same community VLAN, but it cannot communicate with the ports in the same isolated VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN.
`promiscuous`	A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN.

Mode Interface Configuration

Examples To configure host mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode private-vlan host
```

To configure promiscuous mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode private-vlan promiscuous
```

To remove promiscuous mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no switchport mode private-vlan promiscuous
```

Related commands switchport private-vlan mapping

switchport mode private-vlan trunk promiscuous

Overview Use this command to enable a port in trunk mode to be a promiscuous port for isolated VLANs.

NOTE: *Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. Private VLAN trunk ports and GVRP are mutually exclusive.*

Use the **no** variant of this command to remove a port in trunk mode as a promiscuous port for isolated VLANs. You must first remove the secondary port, or ports, in trunk mode associated with the promiscuous port with the **no switchport mode private-vlan trunk secondary** command.

Syntax

```
switchport mode private-vlan trunk promiscuous group <group-id>
no switchport mode private-vlan trunk promiscuous
```

Parameter	Description
<group-id>	The group ID is a numeric value in the range 1 to 32 that is used to associate the promiscuous port with secondary ports.

Default By default, a port in trunk mode is disabled as a promiscuous port.

Mode Interface Configuration

Usage notes A port must be put in trunk mode with switchport mode trunk command before it can be enabled as a promiscuous port.

To add VLANs to be trunked over the promiscuous port, use the switchport trunk allowed vlan command. These VLANs can be isolated VLANs, or non-private VLANs.

To configure the native VLAN for the promiscuous port, use the switchport trunk native vlan command. The native VLAN can be an isolated VLAN, or a non-private VLAN.

When you enable a promiscuous port, all of the secondary port VLANs associated with the promiscuous port via the group ID number must be added to the promiscuous port. In other words, the set of VLANs on the promiscuous port must be a superset of all the VLANs on the secondary ports within the group.

Examples

To create the isolated VLANs 2, 3 and 4 and then enable port1.0.2 in trunk mode as a promiscuous port for these VLANs with the group ID of 3, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2-4
awplus(config-vlan)# private-vlan 2 isolated
awplus(config-vlan)# private-vlan 3 isolated
awplus(config-vlan)# private-vlan 4 isolated
awplus(config-vlan)# exit
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 2-4
awplus(config-if)# switchport mode private-vlan trunk
promiscuous group 3
```

To remove port1.0.2 in trunk mode as a promiscuous port for a private VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport mode private-vlan trunk
promiscuous
```

Note that you must remove the secondary port or ports enabled as trunk ports that are associated with the promiscuous port before removing the promiscuous port.

Related commands

switchport mode private-vlan trunk secondary

switchport mode trunk

switchport trunk allowed vlan

switchport trunk native vlan

show vlan private-vlan

switchport mode private-vlan trunk secondary

Overview Use this command to enable a port in trunk mode to be a secondary port for isolated VLANs.

NOTE: *Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. Private VLAN trunk ports and GVRP are mutually exclusive.*

Use the **no** variant of this command to remove a port in trunk mode as a secondary port for isolated VLANs.

Syntax

```
switchport mode private-vlan trunk secondary group <group-id>
no switchport mode private-vlan trunk secondary
```

Parameter	Description
<group-id>	The group ID is a numeric value in the range 1 to 32 that is used to associate a secondary port with its promiscuous port.

Default By default, a port in trunk mode is disabled as a secondary port.

When a port in trunk mode is enabled to be a secondary port for isolated VLANs, by default it will have a native VLAN of **none** (no native VLAN specified).

Mode Interface Configuration

Usage notes A port must be put in trunk mode with switchport mode trunk command before the port is enabled as a secondary port in trunk mode.

To add VLANs to be trunked over the secondary port use the switchport trunk allowed vlan command. These must be isolated VLANs and must exist on the associated promiscuous port.

To configure the native VLAN for the secondary port, use the switchport trunk native vlan command. The native VLAN must be an isolated VLAN and must exist on the associated promiscuous port.

Examples

To create isolated private VLAN 2 and then enable port1.0.3 in trunk mode as a secondary port for the this VLAN with the group ID of 3, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2
awplus(config-vlan)# private-vlan 2 isolated
awplus(config-vlan)# exit
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 2
awplus(config-if)# switchport mode private-vlan trunk secondary
group 3
```

To remove port1.0.3 in trunk mode as a secondary port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no switchport mode private-vlan trunk
secondary
```

Related commands

switchport mode private-vlan trunk promiscuous

switchport mode trunk

switchport trunk allowed vlan

switchport trunk native vlan

show vlan private-vlan

switchport mode private-vlan ufo

Overview Use this command to allow private VLAN UFO 802.1q member ports to be configured as upstream or downstream.

Use the **no** variant of this command to change the role of the private VLAN UFO 802.1q member port to downstream.

Syntax

```
switchport mode private-vlan ufo <vid-list>
{primary-upstream|secondary-upstream|stp|epsr}
```

```
no switchport mode private-vlan ufo <vid-list>
```

Parameter	Description
<vid-list>	A hyphen-separated range or a comma-separated list of VLAN IDs, all of which must have previously been configured with the private-vlan setting of "ufo".
`primary-upstream`	The primary interface port/LAG that this UFO VLAN will attempt to use as the Upstream interface. More than one primary-upstream interface can be configured.
`secondary-upstream`	The interface that this UFO VLAN will revert to use as the Upstream port if all the primary-upstream ports are unavailable due to being either operationally down (i.e. Link Down) or blocked from forwarding (e.g. STP). More than one secondary-upstream interface can be configured.
`stp`	Let STP determine whether this interface is upstream or downstream. STP will determine if this interface plays the role of an STP Root Port for the CIST, or for the MSTI that this UFO VLAN belongs to. If it is, then UFO will designate this interface as an Upstream interface member for this UFO VLAN. Otherwise it is Downstream.
`epsr`	Let EPSR determine whether this interface is upstream or downstream. If this UFO VLAN is a protected data VLAN in an EPSR instance, and this interface is one of the transit node's interfaces, then this interface will determine if an EPSR Master is reachable from this interface. If it is, then UFO will designate this interface as an Upstream interface member for this UFO VLAN. Otherwise it is Downstream.

Default Downstream.

Note: The default setting for a private VLAN UFO member interface is downstream, but it is not explicitly configured. Use the **no** variant of this command to make the member interface downstream.

Mode Interface Configuration

Example

To configure a private VLAN UFO trunk port as primary-upstream, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 100
awplus(config-if)# switchport mode private-vlan ufo 100
primary-upstream
```

To change the role of the private VLAN UFO 802.1q member port back to the default of downstream, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport mode private-vlan ufo 100
```

Related commands

private-vlan

show vlan private-vlan ufo

Command changes

Version 5.4.7-2.1: command added

Version 5.4.8-2.1: added to SBx8100 Series products

Version 5.4.9-0.1: added to x530 Series products

switchport mode trunk

Overview Use this command to set the switching characteristics of the port to trunk. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Syntax

```
switchport mode trunk [ingress-filter {enable|disable}]
```

Parameter	Description
`ingress-filter`	Set the ingress filtering for the frames received.
`enable`	Turn on ingress filtering for received frames. This is the default.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default By default, ports are in access mode, are untagged members of the default VLAN (VLAN 1), and have ingress filtering on.

Mode Interface Configuration

Usage notes A port in trunk mode can be a tagged member of multiple VLANs, and an untagged member of one native VLAN.

To configure which VLANs this port will trunk for, use the switchport trunk allowed vlan command.

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode trunk ingress-filter enable
```

Related Commands show interface switchport

Command changes Version 5.5.0-1.3: Support for up to 5 VLANs added to AR1050V

switchport private-vlan host-association

Overview Use this command to associate a primary VLAN and a secondary VLAN to a host port. Only one primary and secondary VLAN can be associated to a host port.

Use the **no** variant of this command to remove the association.

Syntax

```
switchport private-vlan host-association <primary-vlan-id> add
<secondary-vlan-id>
```

```
no switchport private-vlan host-association
```

Parameter	Description
<primary-vlan-id>	VLAN ID of the primary VLAN.
<secondary-vlan-id>	VLAN ID of the secondary VLAN (either isolated or community).

Mode Interface Configuration

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport private-vlan host-association 2
add 3
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport private-vlan host-association
```

switchport private-vlan mapping

Overview Use this command to associate a primary VLAN and a set of secondary VLANs to a promiscuous port.

Use the **no** variant of this to remove all the association of secondary VLANs to primary VLANs for a promiscuous port.

Syntax

```
switchport private-vlan mapping <primary-vlan-id> add
<secondary-vid-list>
```

```
switchport private-vlan mapping <primary-vlan-id> remove
<secondary-vid-list>
```

```
no switchport private-vlan mapping
```

Parameter	Description
<primary-vlan-id>	VLAN ID of the primary VLAN.
<secondary-vid-list>	VLAN ID of the secondary VLAN (either isolated or community), or a range of VLANs, or a comma-separated list of VLANs and ranges.

Mode Interface Configuration

Usage notes This command can be applied to a switch port or a static channel group, but not a dynamic (LACP) channel group. LACP channel groups (dynamic/LACP aggregators) cannot be promiscuous ports in private VLANs.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport private-vlan mapping 2 add 3-4
awplus(config-if)# switchport private-vlan mapping 2 remove 3-4
awplus(config-if)# no switchport private-vlan mapping
```

Related commands switchport mode private-vlan

switchport trunk allowed vlan

Overview Use this command to add VLANs to be trunked over this switch port. Traffic for these VLANs can be sent and received on the port.

Use the **no** variant of this command to reset switching characteristics of a specified interface to negate a trunked configuration specified with **switchport trunk allowed vlan** command.

Syntax

```
switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add <vid-list>
switchport trunk allowed vlan remove <vid-list>
switchport trunk allowed vlan except <vid-list>
no switchport trunk
```

Parameter	Description
`all`	Allow all VLANs to transmit and receive through the port.
`none`	Allow no VLANs to transmit and receive through the port.
`add`	Add a VLAN to the list of VLANs that are allowed to transmit and receive through the port. Only use this parameter if a list of VLANs is already configured on a port.
`remove`	Remove a VLAN from the list of VLANs that are allowed to transmit and receive through the port. Only use this parameter if a list of VLANs is already configured on a port. If you are removing VLAN port membership for a large number of switchports and VLANs, note that this command may take a number of minutes to run.
`except`	All VLANs, except the VLAN for which the VID is specified, are part of its port member set. Only use this parameter to remove VLANs after either this parameter or the **all** parameter have added VLANs to a port.
<vid-list>	<2-4094> The ID of the VLAN or VLANs that will be added to, or removed from, the port. A single VLAN, VLAN range, or comma-separated VLAN list can be set. For a VLAN range, specify two VLAN numbers: lowest, then highest number in the range, separated by a hyphen. For a VLAN list, specify the VLAN numbers separated by commas. Do not enter spaces between hyphens or commas when setting parameters for VLAN ranges or lists.

Default By default, ports are untagged members of the default VLAN (VLAN 1).

Mode Interface Configuration

Usage notes

The **all** parameter sets the port to be a tagged member of all the VLANs configured on the device. The **none** parameter removes all VLANs from the port's tagged member set. The **add** and **remove** parameters will add and remove VLANs to and from the port's member set. The **except** parameter creates an exception to the list.

If you use the **all** parameter, and then you want to remove VLANs from the port's member list, you must use the **except** parameter to remove the unwanted VLANs. Similarly, if you use the **except** parameter to remove a list of VLANs, and you want to change that list, you must use the **except** parameter to make that change (not the **add** and **remove** parameters).

For example, if you want to remove VLAN3-5 from a port and the port's configuration is currently **switchport trunk allowed vlan all**, then you should remove VLAN3-5 by entering the **except** parameter, instead of using the **remove** parameter. This means using the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# switchport trunk allowed vlan except 3-5
```

If you do this, then the configuration changes to:

```
awplus#show running-config
interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 3-5
```

For example, if you want to add VLAN4 back in again, and the port configuration is currently **switchport trunk allowed vlan except 3-5**, then you should add VLAN4 by re-entering the **except** parameter with the list of VLANs to remove, instead of using the **add** parameter. This means using the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# switchport trunk allowed vlan except 3,5
```

If you do this, then the configuration changes to:

```
awplus#show running-config
interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 3,5
```

Examples

The following shows adding a single VLAN to a port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2
```

The following shows adding a range of VLANs to a port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2-4
```

The following shows adding a list of VLANs to a port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2,3,4
```

Command changes

Version 5.5.0-1.3: Support for up to 5 VLANs added to AR1050V

switchport trunk native vlan

Overview Use this command to configure the native VLAN for this port. The native VLAN is used for classifying the incoming untagged packets. Use the **none** parameter with this command to remove the native VLAN from the port and set the acceptable frame types to VLAN-tagged only.

Use the **no** variant of this command to reset the native VLAN to the default VLAN ID 1 and remove tagged VLANs from the port.

Syntax

```
switchport trunk native vlan {<vid>|none}
no switchport trunk native vlan
```

Parameter	Description
<vid>	The ID of the VLAN that will be used to classify the incoming untagged packets, in the range 2-2094. The VLAN ID must be a part of the VLAN member set of the port.
none	No native VLAN specified. This option removes the native VLAN from the port and sets the acceptable frame types to vlan-tagged only. Note: Use the **no** variant of this command to revert to the default VLAN 1 as the native VLAN for the specified interface switchport - not **none**.

Default VLAN 1 (the default VLAN), which is reverted to using the **no** form of this command.

Mode Interface Configuration

Examples To set the native VLAN on interface port1.0.2 to VLAN 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk native vlan 2
```

To remove the native VLAN from interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk native vlan none
```

To reset the native VLAN on interface port1.0.2 to the default VLAN 1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport trunk native vlan
```

Command changes Version 5.5.0-1.3: Support for up to 5 VLANs added to AR1050V

switchport vlan translation

Overview Use this command to configure a VLAN translation entry on an interface that supports tagged packets. Create an entry to set either:

- VLAN ID translation: This sets the port to translate a packet's VLAN ID between the one seen on the wire and an internal VID.
- VLAN double-tagging: This enables VLAN double-tagging on the port and specifies the outer-tag VID to be added to packets received on the port. (VLAN double-tagging is also known as VLAN stacking, nested VLANs, or Q-in-Q.)
- Both VLAN ID translation and VLAN double tagging: This both adds an outer-tag VID and translates the inner-tag VID between the wire-VID and the internal VID.

You can create multiple translation entries for a port.

Use the **no** variant of this command to remove all translation entries or a specific entry.

Syntax

```
switchport vlan translation vlan <wire-vid> vlan <vid>
switchport vlan translation vlan <wire-vid> outer-vlan <outer-tag-vid>
switchport vlan translation vlan <wire-vid> vlan <vid> outer-vlan <outer-tag-vid>
no switchport vlan translation [all|vlan <wire-vid>]
```

Parameter	Description
`vlan <wire-vid>`	VLAN-ID of the packet as it is seen on the wire.
`vlan <vid>`	VLAN-ID of the VLAN as it was assigned when the VLAN was created.
`outer-vlan <outer-tag-vid>`	Enable double-tagging with the specified VID as the outer tag.
`all`	Delete all translation entries.

Default None (By default, no translation entries exist.)

Mode Interface Configuration for a switch port, a static channel group, or a dynamic (LACP) channel group. Switch ports must be trunked.

Usage notes This command configures trunked ports only. One or more translation entries can be added to a port. For information on double-tagging on access ports, and for more information about VLAN ID translation and VLAN double-tagging on trunk ports, see the VLAN Feature Overview and Configuration Guide.

NOTE: *VLAN ID translation and VLAN double-tagging cannot be used on the same port in combination with CoS remarking.*

Example

To translate between internal VLAN100 and wire-VID 200 on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport vlan translation vlan 200 vlan 100
```

To add a translation entry to port1.0.1 for wire-VID 200 to add an outer-tag VID of 300 to packets received on the switch port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport vlan translation vlan 200 outer-vlan 300
```

To add a translation entry to port1.0.1 for wire-VID 200 to translate between it and an internal VID of 100 and to add an outer-tag VID of 300, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport vlan translation vlan 200 vlan 100 outer-vlan 300
```

To remove a translation entry from port1.0.1 for wire-VID 200, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no switchport vlan translation vlan 200
```

To remove all translation entries from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no switchport vlan translation all
```

Related commands

show interface switchport vlan translation

switchport mode trunk

switchport vlan translation default drop

Command changes

Version 5.4.8-0.2: added to SBx908 GEN2, x930 Series products

Version 5.4.8-1.1: added to SBx8100 Series products

Version 5.4.9-0.1: added to x530 Series products

Version 5.4.9-1.1: added **outer-vlan** parameter for SBx908 GEN2, x950, x930, x510, x510L, IE510-28GSX and IE300 Series switches.

Version 5.5.0-2.1: added **outer-vlan** parameter for x530 Series switches.

switchport vlan translation default drop

Overview Use this command to drop inbound tagged packets if their VLAN-ID does not match any entries in the VLAN translation table for an interface.

Use the **no** variant of this command to stop dropping non-matching inbound packets and let them be accepted as is for further processing.

Syntax

```
switchport vlan translation default drop
no switchport vlan translation default drop
```

Default Do not drop packets

Mode Interface Configuration for a switch port or a static channel group, or a dynamic (LACP) channel group. The interface must be in a mode that supports tagged packets.

Example To drop inbound tagged packets arriving at port1.0.1 unless they match a VLAN translation entry, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport vlan translation default drop
```

To accept inbound tagged packets arriving at port1.0.1 regardless of whether they match a VLAN translation entry, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no switchport vlan translation default drop
```

Related commands show interface switchport vlan translation

switchport vlan translation

Command changes Version 5.4.8-0.2: added to SBx908 GEN2, x930 Series products

Version 5.4.8-1.1: added to SBx8100 Series products

Version 5.4.9-0.1: added to x530 Series products

switchport vlan-stacking (double-tagging)

Overview Use this command to enable VLAN stacking on a port and set it to be a customer-edge-port or provider-port. This is sometimes referred to as VLAN double-tagging, nested VLANs, or Q in Q.

Use **no** parameter with this command to disable VLAN stacking on an interface.

The port must be in access mode.

Syntax

```
switchport vlan-stacking {customer-edge-port|provider-port}
no switchport vlan-stacking
```

Parameter	Description
`customer-edge-port`	Set the port to be a customer edge port. This port must already be in access mode.
`provider-port`	Set the port to be a provider port. This port must already be in trunk mode.

Default By default, ports are not VLAN stacking ports.

Mode Interface Configuration

Usage Use VLAN stacking to separate traffic from different customers to that they can be managed over a provider network.

This command configures VLAN stacking on ports in access mode. For more information about how to configure this feature, and for information about how to configure VLAN double-tagging (VLAN stacking) on trunk ports, see the VLAN Feature Overview and Configuration Guide.

Note that you must also set an MRU of 1504 or higher on the customer edge port, using the mru command.

Traffic with an extra VLAN header added by VLAN stacking cannot be routed.

Example To apply vlan-stacking to the selected port, configure it to be a customer edge port, and increase the MRU, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport vlan-stacking customer-edge-port
awplus(config-if)# mru 10240
```

Related commands mru

switchport voice dscp

Overview Use this command for a specific port to configure the Layer 3 DSCP value advertised when the transmission of LLDP-MED Network Policy TLVs for voice devices is enabled. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified DSCP value.

Use the **no** variant of this command to reset the DSCP value to the default, 0.

Syntax

```
switchport voice dscp <0-63>
no switchport voice dscp
```

Parameter	Description
`dscp`	Specify a DSCP value for voice data.
<0-63>	DSCP value.

Default A DSCP value of 0 will be advertised.

Mode Interface Configuration

Usage notes LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (lldp run command)
- Voice VLAN is configured for the port (switchport voice vlan command)
- The port is configured to transmit LLDP advertisements—enabled by default (lldp transmit receive command)
- The port is configured to transmit Network Policy TLVs—enabled by default (lldp med-tlv-select command)
- There is an LLDP-MED device connected to the port

Example To tell IP phones connected to port1.0.2 to send voice data with DSCP value 27, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport voice dscp 27
```

Related commands

lldp med-tlv-select

show lldp

switchport voice vlan

switchport voice vlan

Overview Use this command to configure the Voice VLAN tagging advertised when the transmission of LLDP-MED Network Policy TLVs for voice endpoint devices is enabled. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified tagging. This command also sets the ports to be spanning tree edge ports, that is, it enables spanning tree portfast on the ports.

Use the **no** variant of this command to remove LLDP-MED network policy configuration for voice devices connected to these ports. This does not change the spanning tree edge port status.

Syntax

```
switchport voice vlan [<vid>|dot1p|dynamic|untagged]
no switchport voice vlan
```

Parameter	Description
`<vid>`	VLAN identifier, in the range 1 to 4094.
`dot1p`	The IP phone should send User Priority tagged packets, that is, packets in which the tag contains a User Priority value, and a VID of 0. (The User Priority tag is also known as the 802.1p priority tag, or the Class of Service (CoS) tag.)
`dynamic`	The VLAN ID with which the IP phone should send tagged packets will be assigned by RADIUS authentication.
`untagged`	The IP phone should send untagged packets.

Default By default, no Voice VLAN is configured, and therefore no network policy is advertised for voice devices.

Mode Interface Configuration

Usage notes LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (lldp run command)
- Voice VLAN is configured for the port using this command (switchport voice vlan)
- The port is configured to transmit LLDP advertisements—enabled by default (lldp transmit receive command)
- The port is configured to transmit Network Policy TLVs—enabled by default (lldp med-tlv-select command)
- There is an LLDP-MED device connected to the port.

To set the priority value to be advertised for tagged frames, use the switchport voice vlan priority command.

If the Voice VLAN details are to be assigned by RADIUS, then the RADIUS server must be configured to send the attribute "Egress-VLANID (56)" or "Egress-VLAN-Name (58)" in the RADIUS Accept message when authenticating a phone attached to this port.

To set these attributes on the local RADIUS server, use the egress-vlan-id command or the egress-vlan-name command.

For more information about configuring authentication for Voice VLAN, see the LLDP Feature Overview and Configuration Guide.

If the ports have been set to be edge ports by the switchport voice vlan command, the **no** variant of this command will leave them unchanged as edge ports. To set them back to their default non-edge port configuration, use the spanning-tree edgeport (RSTP and MSTP) command.

Examples To tell IP phones connected to port1.0.4 to send voice data tagged for VLAN 10, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# switchport voice vlan 10
```

To tell IP phones connected to port1.0.2-port1.0.8 to send priority tagged packets (802.1p priority tagged with VID 0, so that they will be assigned to the port VLAN) use the following commands. The priority value is 5 by default, but can be configured with the switchport voice vlan priority command.

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.8
awplus(config-if)# switchport voice vlan dot1p
```

To dynamically configure the VLAN ID advertised to IP phones connected to port1.0.1 based on the VLAN assigned by RADIUS authentication (with RADIUS attribute "Egress- VLANID" or "Egress-VLAN-Name" in the RADIUS accept packet), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport voice vlan dynamic
```

To remove the Voice VLAN, and therefore disable the transmission of LLDP-MED network policy information for voice devices on port1.0.8, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.8
awplus(config-if)# no switchport voice vlan
```

Related commands switchport voice dscp

switchport voice vlan priority

switchport voice vlan priority

Overview Use this command to configure the Layer 2 user priority advertised when the transmission of LLDP-MED Network Policy TLVs for voice devices is enabled. This is the priority in the User Priority field of the IEEE 802.1Q VLAN tag, also known as the Class of Service (CoS), or 802.1p priority. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified priority.

Syntax

```
switchport voice vlan priority <0-7>
no switchport voice vlan priority
```

Parameter	Description
`priority`	Specify a user priority value for voice data.
<0-7>	Priority value.

Default By default, the Voice VLAN user priority value is 5.

Mode Interface Configuration

Usage LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (lldp run command)
- Voice VLAN is configured for the port (switchport voice vlan command)
- The port is configured to transmit LLDP advertisements—enabled by default (lldp transmit receive command)
- The port is configured to transmit Network Policy TLVs—enabled by default (lldp med-tlv-select command)
- There is an LLDP-MED device connected to the port.

To set the Voice VLAN tagging to be advertised, use the switchport voice vlan command.

Example To remove the Voice VLAN, and therefore disable the transmission of LLDP-MED network policy information for voice devices on port1.0.6, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no switchport voice vlan
```

Related commands

lldp med-tlv-select

show lldp

switchport voice vlan

vlan

Overview This command creates VLANs, assigns names to them, and enables or disables them. Disabling the VLAN causes all forwarding over the specified VLAN ID to cease. Enabling the VLAN allows forwarding of frames on the specified VLAN.

You can create a management-only VLAN that contains only one member port and may be used as a remote management port. Management-only VLANs process packets in the CPU rather than in hardware. See the parameter table below for more detail.

If you need to control ingress and egress traffic to and from management interfaces, you can use software-based ACLs to filter traffic to and from a management-only VLAN.

The **no** variant of this command destroys the specified VLANs or returns their MTU to the default.

Syntax

```
vlan <vid> [name <vlan-name>] [state
{enable|disable|management-only}]
vlan <vid-range> [state {enable|disable|management-only}]
vlan {<vid>|<vlan-name>} [mtu <mtu-value>]
no vlan {<vid>|<vid-range>} [mtu]
```

Parameter	Description
<vid>	The VID of the VLAN to enable or disable, in the range 1-4094.
<vlan-name>	The ASCII name of the VLAN. Maximum length: 32 characters.
<vid-range>	Specifies a range of VLAN identifiers.
<mtu-value>	Specifies the Maximum Transmission Unit (MTU) size in bytes, in the range 68 to 1500 bytes, for the VLAN.
`enable`	Puts the VLAN into an enabled state.
`disable`	Puts the VLAN into a disabled state.
`management-only`	Management-only VLANs are VLANs which: • have one and only one access port (no aggregators, trunk port etc.) • do not route to/from other interfaces. • process packets in the CPU, rather than in hardware. • cannot be converted to a normal VLAN, nor can a normal VLAN be converted to a management-only VLAN. Delete and re-create the VLAN to convert a normal VLAN to/from a management-only VLAN.

Default By default, VLANs are enabled when they are created.

Mode VLAN Configuration

Examples

To enable VLAN 45, use the commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 45 name accounts state enable
```

To destroy VLAN 45, use the commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 45
```

To create a management-only VLAN with VID 100, use the commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 100 state management-only
```

Related commands

mtu

vlan database

show vlan

Command changes

Version 5.4.9-2.1: Parameter **management-only** added

Version 5.5.0-1.3: Support for up to 5 VLANs added to AR1050V

vlan access-map

Overview Use this command to create a VLAN access-map and enter into VLAN access-map mode, so you can add ACLs to the map. You can use any IPv4 or IPv6 hardware ACLs. VLAN access-maps are used to attach ACLs to VLANs, and therefore to filter traffic as it ingresses VLANs.

See the ACL Feature Overview and Configuration Guide for more information, including information about the number of rules consumed by per-VLAN ACLs, and ACL processing order.

Use the **no** variant of this command to delete a VLAN access-map.

Syntax

```
vlan access-map <name>
no vlan access-map <name>
```

Parameter	Description
<name>	A name for the access-map.

Default By default, no VLAN access-maps exist.

Mode Global Configuration

Example To apply ACL 3001 to VLAN 48, where the ACL drops IP traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 3001 deny ip any any
awplus(config)# vlan access-map deny_all
awplus(config-vlan-access-map)# match access-group 3001
awplus(config-vlan-access-map)# exit
awplus(config)# vlan filter deny_all vlan-list 48 input
```

Related commands

match access-group

show vlan access-map

vlan filter

Command changes Version 5.4.6-2.1: command added

vlan classifier activate

Overview Use this command in Interface Configuration mode to associate a VLAN classifier group with the switch port.

Use the **no** variant of this command to remove the VLAN classifier group from the switch port.

Syntax

```
vlan classifier activate <vlan-class-group-id>
no vlan classifier activate <vlan-class-group-id>
```

Parameter	Description
<vlan-class-group-id>	Specify a VLAN classifier group identifier in the range <1-16>.

Mode Interface Configuration mode for a switch port or link aggregator.

Usage notes See the protocol-based VLAN configuration example in the VLAN Feature Overview and Configuration Guide for configuration details.

Example To associate VLAN classifier group 3 with switch port1.0.3, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# vlan classifier activate 3
```

To remove VLAN classifier group 3 from switch port1.0.3, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no vlan classifier activate 3
```

Related commands

show vlan classifier rule

vlan classifier group

vlan classifier rule ipv4

vlan classifier rule proto

vlan classifier group

Overview Use this command to create a group of VLAN classifier rules. The rules must already have been created.

Use the **no** variant of this command to delete a group of VLAN classifier rules.

Syntax

```
vlan classifier group <1-16> {add|delete} rule
<vlan-class-rule-id>
```

```
no vlan classifier group <1-16>
```

Parameter	Description
<1-16>	VLAN classifier group identifier
`add`	Add the rule to the group.
`delete`	Delete the rule from the group.
<vlan-class-rule-id>	The VLAN classifier rule identifier.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# vlan classifier group 3 add rule 5
```

Related commands

show vlan classifier rule

vlan classifier activate

vlan classifier rule ipv4

vlan classifier rule proto

vlan classifier rule ipv4

Overview Use this command to create an IPv4 subnet-based VLAN classifier rule and map it to a specific VLAN. Use the **no** variant of this command to delete the VLAN classifier rule.

Syntax

```
vlan classifier rule <1-256> ipv4 <ip-addr/prefix-length> vlan <1-4094>
no vlan classifier rule <1-256>
```

Parameter	Description
<1-256>	Specify the VLAN Classifier Rule identifier.
<ip-addr/prefix-length>	Specify the IP address and prefix length.
<1-4094>	Specify a VLAN ID to which an untagged packet is mapped in the range *<1-4094>*.

Mode Global Configuration

Usage notes If the source IP address matches the IP subnet specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN.

NOTE: *The subnet VLAN classifier only matches IPv4 packets. It does not match ARP packets. To ensure ARP traffic is classified into the correct subnet VLAN, you can use a hardware based policy map that sends ARP packets to the CPU, which will then process them appropriately. This means that if you use subnet-based VLANs, you should also configure the following:*

NOTE: *The policy map should be applied to each port that uses a subnet based VLAN using the service-policy input command:*

Example

```
awplus# configure terminal
awplus(config)# vlan classifier rule 3 ipv4 3.3.3.3/8 vlan 5
```

Related commands

show vlan classifier rule

vlan classifier activate

vlan classifier rule proto

vlan classifier rule proto

Overview Use this command to create a protocol type-based VLAN classifier rule, and map it to a specific VLAN. See the published IANA EtherType IEEE 802 numbers here:

www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt.

Instead of a protocol name the decimal value of the protocol's EtherType can be entered. The EtherType field is a two-octet field in an Ethernet frame. It is used to show which protocol is encapsulated in the payload of the Ethernet frame. Note that EtherTypes in the IANA 802 numbers are given as hexadecimal values.

The **no** variant of this command removes a previously set rule.

Syntax

```
vlan classifier rule <1-256> proto <protocol> encap
{ethv2|nosnapllc|snapllc} vlan <1-4094>
```

```
no vlan classifier rule <1-256>
```

Parameter	Description	
<1-256>	VLAN Classifier identifier	
proto	Protocol type	
<protocol>	Specify a protocol either by its decimal number (0-65535) or by one of the following protocol names:	
	[arp|2054]	Address Resolution protocol
	[atalkaarp|33011]	Appletalk AARP protocol
	[atalkddp|32923]	Appletalk DDP protocol
	[atmmulti|34892]	MultiProtocol Over ATM protocol
	[atmtransport|34948]	Frame-based ATM Transport protocol
	[dec|24576]	DEC Assigned protocol
	[deccustom|24582]	DEC Customer use protocol
	[decdiagnostics|24581]	DEC Systems Comms Arch protocol
	[decdnadumpload|24577]	DEC DNA Dump/Load protocol
	[decdnaremoteconsole|24578]	DEC DNA Remote Console protocol
	[decdnarouting|24579]	DEC DNA Routing protocol
	[declat|24580]	DEC LAT protocol

Parameter	Description	
	`[decsyscomm|24583]`	DEC Systems Comms Arch protocol
	`[g8bpqx25|2303]`	G8BPQ AX.25 protocol
	`[ieeeaddrtrans|2561]`	Xerox IEEE802.3 PUP Address
	`[ieeepup|2560]`	Xerox IEEE802.3 PUP protocol
	`[ip|2048]`	IP protocol
	`[ipv6|34525]`	IPv6 protocol
	`[ipx|33079]`	IPX protocol
	`[netbeui|61680]`	IBM NETBIOS/NETBEUI protocol
	`[netbeui|61681]`	IBM NETBIOS/NETBEUI protocol
	`[pppdiscovery|34915]`	PPPoE discovery protocol
	`[pppsession|34916]`	PPPoE session protocol
	`[rarp|32821]`	Reverse Address Resolution protocol
	`[x25|2056]`	CCITT.25 protocol
	`[xeroxaddrtrans|513]`	Xerox PUP Address Translation protocol
	`[xeroxpup|512]`	Xerox PUP protocol
`ethv2`	Ethernet Version 2 encapsulation	
`nosnapllc`	LLC without SNAP encapsulation	
`snapllc`	LLC SNAP encapsulation	
<1-4094>	Specify a VLAN ID to which an untagged packet is mapped in the range *<1-4094>*	

Mode Global Configuration

Usage notes If the protocol type matches the protocol specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN. Ethernet Frame Numbers may be entered in place of the protocol names listed. For a full list please refer to the IANA list online:
www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt

Example

```
awplus# configure terminal
awplus(config)# vlan classifier rule 1 proto x25 encap ethv2 vlan 2
awplus(config)# vlan classifier rule 2 proto 512 encap ethv2 vlan 2
awplus(config)# vlan classifier rule 3 proto 2056 encap ethv2 vlan 2
awplus(config)# vlan classifier rule 4 proto 2054 encap ethv2 vlan 2
```

Validation Output

```
awplus# show vlan classifier rule
```

```
vlan classifier rule 16 proto rarp encap ethv2 vlan 2

vlan classifier rule 8 proto encap ethv2 vlan 2

vlan classifier rule 4 proto arp encap ethv2 vlan 2

vlan classifier rule 3 proto xeroxpup encap ethv2 vlan 2
vlan classifier rule 2 proto ip encap ethv2 vlan 2
vlan classifier rule 1 proto ipv6 encap ethv2 vlan 2
```

Related commands

show vlan classifier rule

vlan classifier activate

vlan classifier group

vlan database

Overview Use this command to enter the VLAN Configuration mode. You can then add or delete a VLAN, or modify its values.

Syntax

```
vlan database
```

Mode Global Configuration

Example In the following example, note the change to VLAN Configuration mode from Global Configuration mode:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)#
```

Related commands vlan

Command changes Version 5.5.0-1.3: Support for up to 5 VLANs added to AR1050V

vlan filter

Overview Use this command to apply a VLAN access-map to a list of VLANs. The switch uses the ACLs in the access-map to filter traffic ingressing those VLANs.

See the ACL Feature Overview and Configuration Guide for more information, including information about the number of rules consumed by per-VLAN ACLs, and ACL processing order.

Use the **no** variant of this command to to remove the access-map filter from the listed VLANs.

Syntax

```
vlan filter <access-map-name> vlan-list <vid> input
no vlan filter <access-map-name> vlan-list <vid> input
```

Parameter	Description
<access-map-name>	The name of the VLAN access-map to apply to the specified list of VLANs
`vlan-list <vid>`	The list of VLANs to filter. You can specify a single VLAN (e.g. 49), a comma-separated list of VLANs (e.g. 49, 51), a hyphenated range of VLANs (e.g. 49-51), or a combination (e.g. 49,51-53)
`input`	Apply the filter to ingress traffic

Default By default, no VLAN filters exist.

Mode Global Configuration

Example To apply ACL 3001 to VLAN 48, where the ACL drops IP traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 3001 deny ip any any
awplus(config)# vlan access-map deny_all
awplus(config-vlan-access-map)# match access-group 3001
awplus(config-vlan-access-map)# exit
awplus(config)# vlan filter deny_all vlan-list 48 input
```

Related commands match access-group

show vlan filter

vlan access-map

Command changes Version 5.4.6-2.1: command added

17 Spanning Tree Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure RSTP, STP or MSTP. For information about spanning trees, including configuration procedures, see the STP Feature Overview and Configuration Guide.

Command List

- "clear spanning-tree statistics" on page 673
- "clear spanning-tree detected protocols (RSTP and MSTP)" on page 674
- "debug mstp (RSTP and STP)" on page 675
- "instance priority (MSTP)" on page 679
- "instance vlan (MSTP)" on page 681
- "region (MSTP)" on page 683
- "revision (MSTP)" on page 684
- "show debugging mstp" on page 685
- "show spanning-tree" on page 686
- "show spanning-tree brief" on page 689
- "show spanning-tree mst" on page 690
- "show spanning-tree mst config" on page 691
- "show spanning-tree mst detail" on page 692
- "show spanning-tree mst detail interface" on page 694
- "show spanning-tree mst instance" on page 696
- "show spanning-tree mst instance interface" on page 697
- "show spanning-tree mst interface" on page 698
- "show spanning-tree statistics" on page 699
- "show spanning-tree statistics instance" on page 701

- "show spanning-tree statistics instance interface" on page 702
- "show spanning-tree statistics interface" on page 704
- "show spanning-tree vlan range-index" on page 706
- "spanning-tree autoedge (RSTP and MSTP)" on page 707
- "spanning-tree bpdu" on page 708
- "spanning-tree cisco-interoperability (MSTP)" on page 710
- "spanning-tree edgeport (RSTP and MSTP)" on page 711
- "spanning-tree enable" on page 712
- "spanning-tree errdisable-timeout enable" on page 714
- "spanning-tree errdisable-timeout interval" on page 715
- "spanning-tree force-version" on page 716
- "spanning-tree forward-time" on page 717
- "spanning-tree guard root" on page 718
- "spanning-tree hello-time" on page 719
- "spanning-tree link-type" on page 720
- "spanning-tree max-age" on page 721
- "spanning-tree max-hops (MSTP)" on page 722
- "spanning-tree mode" on page 723
- "spanning-tree mst configuration" on page 724
- "spanning-tree mst instance" on page 725
- "spanning-tree mst instance path-cost" on page 726
- "spanning-tree mst instance priority" on page 728
- "spanning-tree mst instance restricted-role" on page 729
- "spanning-tree mst instance restricted-tcn" on page 731
- "spanning-tree path-cost" on page 732
- "spanning-tree portfast (STP)" on page 733
- "spanning-tree portfast bpdu-filter" on page 735
- "spanning-tree portfast bpdu-guard" on page 737
- "spanning-tree priority (bridge priority)" on page 739
- "spanning-tree priority (port priority)" on page 740
- "spanning-tree restricted-role" on page 741
- "spanning-tree restricted-tcn" on page 742
- "spanning-tree transmit-holdcount" on page 743
- "undebug mstp" on page 744

clear spanning-tree statistics

Overview Use this command to clear all the STP BPDU (Bridge Protocol Data Unit) statistics.

Syntax

```
clear spanning-tree statistics
clear spanning-tree statistics [instance <mstp-instance>]
clear spanning-tree statistics [interface <port> [instance
<mstp-instance>]]
```

Parameter	Description
<port>	The port to clear STP BPDU statistics for. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).
<mstp-instance>	The MSTP instance (MSTI - Multiple Spanning Tree Instance) to clear MSTP BPDU statistics.

Mode User Exec and Privileged Exec

Usage notes Use this command with the **instance** parameter in MSTP mode. Specifying this command with the **interface** parameter only not the instance parameter will work in STP and RSTP mode.

Examples

```
awplus# clear spanning-tree statistics
awplus# clear spanning-tree statistics instance 1
awplus# clear spanning-tree statistics interface port1.0.2
awplus# clear spanning-tree statistics interface port1.0.2
instance 1
```

clear spanning-tree detected protocols (RSTP and MSTP)

Overview Use this command to clear the detected protocols for a specific port, or all ports.

Use this command in RSTP or MSTP mode only.

Syntax

```
clear spanning-tree detected protocols [interface <port>]
```

Parameter	Description
<port>	The port to clear detected protocols for. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode Privileged Exec

Example

```
awplus# clear spanning-tree detected protocols
```

debug mstp (RSTP and STP)

Overview Use this command to enable debugging for the configured spanning tree mode, and echo data to the console, at various levels. Note that although this command uses the keyword **mstp** it displays debugging output for RSTP and STP protocols as well the MSTP protocol.

Use the **no** variant of this command to disable spanning tree debugging.

Syntax

```
debug mstp {all|cli|protocol [detail]|timer [detail]}
debug mstp {packet {rx|tx} [decode] [interface <interface>]}
debug mstp {topology-change [interface <interface>]}
no debug mstp {all|cli|protocol [detail]|timer [detail]}
no debug mstp {packet {rx|tx} [decode] [interface <interface>]}
no debug mstp {topology-change [interface <interface>]}
```

Parameter	Description
`all`	Echoes all spanning tree debugging levels to the console.
`cli`	Echoes spanning tree commands to the console.
`packet`	Echoes spanning tree packets to the console.
`rx`	Received packets.
`tx`	Transmitted packets.
`protocol`	Echoes protocol changes to the console.
`timer`	Echoes timer information to the console.
`detail`	Detailed output.
`decode`	Interprets packet contents
`topology-change`	Interprets topology change messages
`interface`	Keyword before <interface> placeholder to specify an interface to debug
<interface>	Placeholder used to specify the name of the interface to debug.

Mode Privileged Exec and Global Configuration mode

Usage 1 Use the **debug mstp topology-change interface** command to generate debugging messages when the device receives an indication of a topology change in a BPDU from another device. The debugging can be activated on a per-port basis. Although this command uses the keyword **mstp**, it displays debugging output for RSTP and STP protocols as well as the MSTP protocol.

Due to the likely volume of output, these debug messages are best viewed using the terminal monitor command before issuing the relevant **debug mstp**

command. The default terminal monitor filter will select and display these messages. Alternatively, the messages can be directed to any of the other log outputs by adding a filter for the MSTP application using log buffered (filter) command:

```
awplus# configure terminal
awplus(config)# log buffered program mstp
```

Output 1

```
awplus#terminal monitor
awplus#debug mstp topology-change interface port1.0.4
10:09:09 awplus MSTP[1409]: Topology change rcvd on port1.0.4 (internal)
10:09:09 awplus MSTP[1409]: Topology change rcvd on MSTI 1 port1.0.4
awplus#debug mstp topology-change interface port1.0.6
10:09:29 awplus MSTP[1409]: Topology change rcvd on port1.0.6 (external)
10:09:29 awplus MSTP[1409]: Topology change rcvd on MSTI 1 port1.0.6
```

Usage 2 Use the **debug mstp packet rx|tx decode interface** command to generate debugging messages containing the entire contents of a BPDU displayed in readable text for transmitted and received xSTP BPDUs. The debugging can be activated on a per-port basis and transmit and receive debugging is controlled independently. Although this command uses the keyword **mstp**, it displays debugging output for RSTP and STP protocols as well as the MSTP protocol.

Due to the likely volume of output, these debug messages are best viewed using the terminal monitor command before issuing the relevant **debug mstp** command. The default terminal monitor filter will select and display these messages. Alternatively, the messages can be directed to any of the other log outputs by adding a filter for the MSTP application using the log buffered (filter) command:

```
awplus(config)# log buffered program mstp
```

Output 2 In MSTP mode - an MSTP BPDU with 1 MSTI:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
17:23:42 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:23:42 awplus MSTP[1417]: Protocol version: MSTP, BPDU type: RST
17:23:42 awplus MSTP[1417]: CIST Flags:  Agree Forward Learn role=Desig
17:23:42 awplus MSTP[1417]: CIST root id      : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST ext pathcost : 0
17:23:42 awplus MSTP[1417]: CIST reg root id  : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST port id      : 8001 (128:1)
17:23:42 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:23:42 awplus MSTP[1417]: Version 3 length : 80
17:23:42 awplus MSTP[1417]: Format id      : 0
17:23:42 awplus MSTP[1417]: Config name    : test
17:23:42 awplus MSTP[1417]: Revision level : 0
17:23:42 awplus MSTP[1417]: Config digest  : 3ab68794d602fdf43b21c0b37ac3bca8
17:23:42 awplus MSTP[1417]: CIST int pathcost : 0
17:23:42 awplus MSTP[1417]: CIST bridge id    : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST hops remaining : 20
17:23:42 awplus MSTP[1417]: MSTI flags           : Agree Forward Learn role=Desig
17:23:42 awplus MSTP[1417]: MSTI reg root id     : 8001:0000cd1000fe
17:23:42 awplus MSTP[1417]: MSTI pathcost        : 0
17:23:42 awplus MSTP[1417]: MSTI bridge priority : 32768 port priority : 128
17:23:42 awplus MSTP[1417]: MSTI hops remaining  : 20
17:23:42 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - finish
```

In STP mode transmitting a TCN BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet tx decode interface port1.0.4
17:28:09 awplus MSTP[1417]: port1.0.4 xSTP BPDU tx - start
17:28:09 awplus MSTP[1417]: Protocol version: STP, BPDU type: TCN
17:28:09 awplus MSTP[1417]: port1.0.4 xSTP BPDU tx - finish
```

In STP mode receiving an STP BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
17:31:36 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:31:36 awplus MSTP[1417]: Protocol version: STP, BPDU type: Config
17:31:36 awplus MSTP[1417]: Flags:  role=none
17:31:36 awplus MSTP[1417]: Root id      : 8000:0000cd1000fe
17:31:36 awplus MSTP[1417]: Root pathcost : 0
17:31:36 awplus MSTP[1417]: Bridge id  : 8000:0000cd1000fe
17:31:36 awplus MSTP[1417]: Port id      : 8001 (128:1)
17:31:36 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:31:36 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - finish
```

In RSTP mode receiving an RSTP BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
awplus#17:30:17 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:30:17 awplus MSTP[1417]: Protocol version: RSTP, BPDU type: RST
17:30:17 awplus MSTP[1417]: CIST Flags:  Forward Learn role=Desig
17:30:17 awplus MSTP[1417]: CIST root id      : 8000:0000cd1000fe
17:30:17 awplus MSTP[1417]: CIST ext pathcost : 0
17:30:17 awplus MSTP[1417]: CIST reg root id  : 8000:0000cd1000fe
17:30:17 awplus MSTP[1417]: CIST port id      : 8001 (128:1)
17:30:17 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:30:17 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - finish
```

Examples

```
awplus# debug mstp all
awplus# debug mstp cli
awplus# debug mstp packet rx
awplus# debug mstp protocol detail
awplus# debug mstp timer
awplus# debug mstp packet rx decode interface port1.0.2
awplus# debug mstp packet tx decode interface port1.0.6
```

Related commands

log buffered (filter)

show debugging mstp

terminal monitor

undebug mstp

instance priority (MSTP)

Overview Use this command to set the priority for this device to become the root bridge for the specified MSTI (Multiple Spanning Tree Instance).

Use this command for MSTP only.

Use the **no** variant of this command to restore the root bridge priority of the device for the instance to the default.

Syntax

```
instance <instance-id> priority <priority>
no instance <instance-id> priority
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<priority>	Specify the root bridge priority for the device for the MSTI in the range <0-61440>. Note that a lower priority number indicates a greater likelihood of the device becoming the root bridge. The priority values can be set only in increments of 4096. If you specify a number that is not a multiple of 4096, it will be rounded down. The default priority is 32768.

Default The default priority value for all instances is 32768.

Mode MST Configuration

Usage notes MSTP lets you distribute traffic more efficiently across a network by blocking different links for different VLANs. You do this by making different devices into the root bridge for each MSTP instance, so that each instance blocks a different link.

If all devices have the same root bridge priority for the instance, MSTP selects the device with the lowest MAC address to be the root bridge. Give the device a higher priority for becoming the root bridge for a particular instance by assigning it a lower priority number, or vice versa.

Examples To set the root bridge priority for MSTP instance 2 to be the highest (0), so that it will be the root bridge for this instance when available, use the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 2 priority 0
```

To reset the root bridge priority for instance 2 to the default (32768), use the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# no instance 2 priority
```

Related commands

region (MSTP)

revision (MSTP)

show spanning-tree mst config

spanning-tree mst instance

spanning-tree mst instance priority

instance vlan (MSTP)

Overview Use this command to create an MST Instance (MSTI), and associate the specified VLANs with it. An MSTI is a spanning tree instance that exists within an MST region (MSTR).

When a VLAN is associated with an MSTI the member ports of the VLAN are automatically configured to send and receive spanning-tree information for the associated MSTI. You can disable this automatic configuration of member ports of the VLAN to the associated MSTI by using a **no spanning-tree mst instance** command to remove the member port from the MSTI.

Use the **instance vlan** command for MSTP only.

Use the **no** variant of this command to remove the specified VLANs from the MSTI.

Syntax

```
instance <instance-id> vlan <vid-list>
no instance <instance-id> vlan <vid-list>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<vid-list>	Specify one or more VLAN identifiers (VID) to be associated with the MSTI specified. This can be a single VID in the range 1-4094, or a hyphen-separated range or a comma-separated list of VLAN IDs.

Mode MST Configuration

Usage notes The VLANs must be created before being associated with an MST instance (MSTI). If the VLAN range is not specified, the MSTI will not be created.

This command removes the specified VLANs from the CIST and adds them to the specified MSTI. If you use the **no** variant of this command to remove the VLAN from the MSTI, it returns it to the CIST. To move a VLAN from one MSTI to another, you must first use the **no** variant of this command to return it to the CIST.

Ports in these VLANs will remain in the control of the CIST until you associate the ports with the MSTI using the spanning-tree mst instance command.

Example To associate VLAN 30 with MSTI 2, use the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 2 vlan 30
```

Related commands

region (MSTP)

revision (MSTP)

show spanning-tree mst config

spanning-tree mst instance

vlan

region (MSTP)

Overview Use this command to assign a name to the device's MST Region. MST Instances (MSTI) of a region form different spanning trees for different VLANs.

Use this command for MSTP only.

Use the **no** variant of this command to remove this region name and reset it to the default.

Syntax

```
region <region-name>
no region
```

Parameter	Description
<region-name>	Specify the name of the region, up to 32 characters. Valid characters are upper-case, lower-case, digits, underscore.

Default By default, the region name is My Name.

Mode MST Configuration

Usage The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

Example

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# region ATL
```

Related commands revision (MSTP)

show spanning-tree mst config

revision (MSTP)

Overview Use this command to specify the MST revision number to be used in the configuration identifier.

Use this command for MSTP only.

Syntax

```
revision <revision-number>
```

Parameter	Description
<revision-number>	<0-65535> Revision number.

Default The default of revision number is 0.

Mode MST Configuration

Usage The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

Example

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# revision 25
```

Related commands

region (MSTP)

show spanning-tree mst config

instance vlan (MSTP)

show debugging mstp

Overview Use this command to see what debugging is turned on for MSTP.

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

Syntax

```
show debugging mstp
```

Mode User Exec and Privileged Exec

Example To display the MSTP debugging options set, enter the command:

```
awplus# show debugging mstp
```

Output Figure 17-1: Example output from **show debugging mstp**

```
MSTP debugging status:
  MSTP receiving packet debugging is on
```

Related commands debug mstp (RSTP and STP)

show spanning-tree

Overview Use this command to display detailed spanning tree information on the specified port or on all ports. Use this command for RSTP, MSTP or STP.

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

Syntax

```
show spanning-tree [interface <port-list>]
```

Parameter	Description
`interface`	Display information about the following port only.
<port-list>	The ports to display information about. A port-list can be: • a switch port (e.g. port1.0.6) a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2) • a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.4, or sa1-2, or po1-2 • a comma-separated list of ports and port ranges, e.g. port1.0.1,port1.0.4-1.0.6. Do not mix switch ports, static channel groups, and dynamic (LACP) channel groups in the same list

Mode User Exec and Privileged Exec

Usage notes Note that any list of interfaces specified must not span any interfaces that are not installed.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the **show spanning-tree** command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

Example To display spanning tree information about port1.0.3, use the command:

```
awplus# show spanning-tree interface port1.0.3
```

Output Figure 17-2: Example output from **show spanning-tree** in RSTP mode

```
awplus#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000000cd24ff2d
% 1: Bridge Id 80000000cd24ff2d
% 1: last topology change Mon Oct 3 02:06:26 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.1: Port 5001 - Id 8389 - Role Disabled - State Discarding
%   port1.0.1: Designated Path Cost 0
%   port1.0.1: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.1: Designated Port Id 8389 - Priority 128  -
%   port1.0.1: Root 80000000cd24ff2d
%   port1.0.1: Designated Bridge 80000000cd24ff2d
%   port1.0.1: Message Age 0 - Max Age 20
%   port1.0.1: Hello Time 2 - Forward Delay 15
%   port1.0.1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   port1.0.1: forward-transitions 0
%   port1.0.1: Version Rapid Spanning Tree Protocol - Received None - Send STP
%   port1.0.1: No portfast configured - Current  portfast off
%   port1.0.1: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.1: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.1: no root guard configured     - Current root guard off
%   port1.0.1: Configured Link Type point-to-point - Current  shared
%
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Path Cost 0
%   port1.0.2: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.2: Designated Port Id 838a - Priority 128  -
%   port1.0.2: Root 80000000cd24ff2d
%   port1.0.2: Designated Bridge 80000000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 20
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   port1.0.2: forward-transitions 0
%   port1.0.2: Version Rapid Spanning Tree Protocol - Received None - Send STP
%   port1.0.2: No portfast configured - Current  portfast off
%   port1.0.2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.2: no root guard configured     - Current root guard off
%   port1.0.2: Configured Link Type point-to-point - Current  shared
```

Output Figure 17-3: Example output from **show spanning-tree**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000000cd20f093
% 1: Bridge Id 80000000cd20f093
% 1: last topology change Mon Oct 3 02:06:26 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.3: Port 5023 - Id 839f - Role Designated - State Forwarding
%   port1.0.3: Designated Path Cost 0
%   port1.0.3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   port1.0.3: Designated Port Id 839f - Priority 128  -
%   port1.0.3: Root 80000000cd20f093
%   port1.0.3: Designated Bridge 80000000cd20f093
%   port1.0.3: Message Age 0 - Max Age 20
%   port1.0.3: Hello Time 2 - Forward Delay 15
%   port1.0.3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   port1.0.3: forward-transitions 32
%   port1.0.3: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   port1.0.3: No portfast configured - Current  portfast off
%   port1.0.3: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.3: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.3: no root guard configured     - Current root guard off
%   port1.0.3: Configured Link Type point-to-point - Current point-to-point
...
```

show spanning-tree brief

Overview Use this command to display a summary of spanning tree status information on all ports. Use this command for RSTP, MSTP or STP.

Syntax

```
show spanning-tree brief
```

Parameter	Description
`brief`	A brief summary of spanning tree information.

Mode User Exec and Privileged Exec

Usage notes Note that any list of interfaces specified must not span any interfaces that are not installed.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the **show spanning-tree** command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

Example To display a summary of spanning tree status information, use the command:

```
awplus# show spanning-tree brief
```

Output Figure 17-4: Example output from **show spanning-tree brief**

```
Default: Bridge up - Spanning Tree Enabled
Default: Root Path Cost 40000 - Root Port 4501 -  Bridge Priority 32768
Default: Root Id 8000:0000cd250001
Default: Bridge Id 8000:0000cd296eb1

Port            Designated Bridge    Port Id    Role          State
sa1             8000:001577c9744b    8195       Rootport      Forwarding
po1             8000:0000cd296eb1    81f9       Designated    Forwarding
port1.0.1       8000:0000cd296eb1    8389       Disabled      Discarding
port1.0.2       8000:0000cd296eb1    838a       Disabled      Discarding
port1.0.3       8000:0000cd296eb1    838b       Disabled      Discarding
...
```

Related commands show spanning-tree

show spanning-tree mst

Overview This command displays bridge-level information about the CIST and VLAN to MSTI mappings.

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

Syntax

```
show spanning-tree mst
```

Mode User Exec, Privileged Exec and Interface Configuration

Example To display bridge-level information about the CIST and VLAN to MSTI mappings, enter the command:

```
awplus# show spanning-tree mst
```

Output Figure 17-5: Example output from **show spanning-tree mst**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000000475e93ffe
% 1: CIST Reg Root Id 8000000475e93ffe
% 1: CST Bridge Id 8000000475e93ffe
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%
%   Instance        VLAN
%   0:              1
%   2:              4
```

Related commands show spanning-tree mst interface

show spanning-tree mst config

Overview Use this command to display MSTP configuration identifier for the device.

Syntax

```
show spanning-tree mst config
```

Mode User Exec, Privileged Exec and Interface Configuration

Usage notes The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

Example To display MSTP configuration identifier information, enter the command:

```
awplus# show spanning-tree mst config
```

Output Figure 17-6: Example output from **show spanning-tree mst config**

```
awplus#show spanning-tree mst config
%
%  MSTP Configuration Information:
%--------------------------------------------------------
%  Format Id      : 0
%  Name           : My Name
%  Revision Level : 0
%  Digest         : 0x80DEE46DA92A98CF21C603291B22880A
%--------------------------------------------------------
```

Related commands

instance vlan (MSTP)

region (MSTP)

revision (MSTP)

show spanning-tree mst detail

Overview This command displays detailed information about each instance, and all interfaces associated with that particular instance.

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

Syntax
```
show spanning-tree mst detail
```

Mode User Exec, Privileged Exec and Interface Configuration

Example To display detailed information about each instance, and all interfaces associated with them, enter the command:

```
awplus# show spanning-tree mst detail
```

Output Figure 17-7: Example output from **show spanning-tree mst detail**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Reg Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.1: Port 5001 - Id 8389 - Role Disabled - State Discarding
%   port1.0.1: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.0.1: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.1: Designated Port Id 8389 - CIST Priority 128  -
%   port1.0.1: CIST Root 80000000cd24ff2d
%   port1.0.1: Regional Root 80000000cd24ff2d
%   port1.0.1: Designated Bridge 80000000cd24ff2d
%   port1.0.1: Message Age 0 - Max Age 20
%   port1.0.1: CIST Hello Time 2 - Forward Delay 15
%   port1.0.1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
...
%   port1.0.2: forward-transitions 0
%   port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   port1.0.2: No portfast configured - Current  portfast off
%   port1.0.2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.2: no root guard configured     - Current root guard off
%   port1.0.2: Configured Link Type point-to-point - Current  shared
%
```

```
%   port1.0.3: Port 5003 - Id 838b - Role Disabled - State Discarding
%   port1.0.3: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.0.3: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.3: Designated Port Id 838b - CIST Priority 128  -
%   port1.0.3: CIST Root 80000000cd24ff2d
%   port1.0.3: Regional Root 80000000cd24ff2d
%   port1.0.3: Designated Bridge 80000000cd24ff2d
%   port1.0.3: Message Age 0 - Max Age 20
%   port1.0.3: CIST Hello Time 2 - Forward Delay 15
%   port1.0.3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
%   port1.0.3: forward-transitions 0
%   port1.0.3: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   port1.0.3: No portfast configured - Current  portfast off
%   port1.0.3: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.3: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.3: no root guard configured     - Current root guard off
%   port1.0.3: Configured Link Type point-to-point - Current  shared
```

show spanning-tree mst detail interface

Overview This command displays detailed information about the specified switch port, and the MST instances associated with it.

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

Syntax

```
show spanning-tree mst detail interface <port>
```

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec, Privileged Exec and Interface Configuration

Example To display detailed information about port1.0.3 and the instances associated with it, enter the command:

```
awplus# show spanning-tree mst detail interface port1.0.3
```

Output Figure 17-8: Example output from **show spanning-tree mst detail interface**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Reg Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.0.2: Configured Path Cost 20000000  - Add type Explicit ref count 2
%   port1.0.2: Designated Port Id 838a - CIST Priority 128  -
%   port1.0.2: CIST Root 80000000cd24ff2d
%   port1.0.2: Regional Root 80000000cd24ff2d
%   port1.0.2: Designated Bridge 80000000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 20
%   port1.0.2: CIST Hello Time 2 - Forward Delay 15
%   port1.0.2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
%   port1.0.2: forward-transitions 0
%   port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
```

```
%   port1.0.2: No portfast configured - Current  portfast off
%   port1.0.2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.2: no root guard configured     - Current root guard off
%   port1.0.2: Configured Link Type point-to-point - Current  shared
%
% Instance  2:  Vlans: 2
% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Internal Path Cost 0  - Designated Port Id 838a
%   port1.0.2: Configured Internal Path Cost 20000000
%   port1.0.2: Configured CST External Path cost 20000000
%   port1.0.2: CST Priority 128  - MSTI Priority 128
%   port1.0.2: Designated Root 80020000cd24ff2d
%   port1.0.2: Designated Bridge 80020000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 0
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

show spanning-tree mst instance

Overview This command displays detailed information for the specified instance, and all switch ports associated with that instance.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the show spanning-tree command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

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

Syntax

```
show spanning-tree mst instance <instance-id>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.

Mode User Exec, Privileged Exec, and Interface Configuration

Example To display detailed information for **instance 2**, and all switch ports associated with that instance, use the command:

```
awplus# show spanning-tree mst instance 2
```

Output Figure 17-9: Example output from **show spanning-tree mst instance**

```
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Internal Path Cost 0  - Designated Port Id 838a
%   port1.0.2: Configured Internal Path Cost 20000000
%   port1.0.2: Configured CST External Path cost 20000000
%   port1.0.2: CST Priority 128  - MSTI Priority 128
%   port1.0.2: Designated Root 80020000cd24ff2d
%   port1.0.2: Designated Bridge 80020000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 0
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

show spanning-tree mst instance interface

Overview This command displays detailed information for the specified MST (Multiple Spanning Tree) instance, and the specified switch port associated with that MST instance.

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

Syntax

```
show spanning-tree mst instance <instance-id> interface <port>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<port>	The port to display information about. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2).

Mode User Exec, Privileged Exec, and Interface Configuration

Example To display detailed information for instance 2, interface port1.0.2, use the command:

```
awplus# show spanning-tree mst instance 2 interface port1.0.2
```

Output Figure 17-10: Example output from **show spanning-tree mst instance**

```
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Internal Path Cost 0  - Designated Port Id 838a
%   port1.0.2: Configured Internal Path Cost 20000000
%   port1.0.2: Configured CST External Path cost 20000000
%   port1.0.2: CST Priority 128  - MSTI Priority 128
%   port1.0.2: Designated Root 80020000cd24ff2d
%   port1.0.2: Designated Bridge 80020000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 0
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

show spanning-tree mst interface

Overview This command displays the number of instances created, and VLANs associated with it for the specified switch port.

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

Syntax

```
show spanning-tree mst interface <port>
```

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec, Privileged Exec, and Interface Configuration

Example To display detailed information about each instance, and all interfaces associated with them, for port1.0.4, use the command:

```
awplus# show spanning-tree mst interface port1.0.4
```

Output Figure 17-11: Example output from **show spanning-tree mst interface**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000008c73a2b22
% 1: CIST Reg Root Id 80000008c73a2b22
% 1: CST Bridge Id 80000008c73a2b22
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
%
%   Instance        VLAN
%   0:              1
%   1:              2-3
%   2:              4-5
```

show spanning-tree statistics

Overview This command displays BPDU (Bridge Protocol Data Unit) statistics for all spanning-tree instances, and all switch ports associated with all spanning-tree instances.

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

Syntax

```
show spanning-tree statistics
```

Mode Privileged Exec

Usage notes To display BPDU statistics for all spanning-tree instances, and all switch ports associated with all spanning-tree instances, use the command:

```
awplus# show spanning-tree statistics
```

Output Figure 17-12: Example output from **show spanning-tree statistics**

```
Port number = 915 Interface = port1.0.6
                ================================
% BPDU Related Parameters
% ------------------------
% Port Spanning Tree                : Disable
% Spanning Tree Type                : Rapid Spanning Tree Protocol
% Current Port State                : Discarding
% Port ID                           : 8393
% Port Number                       : 393
% Path Cost                         : 20000000
% Message Age                       : 0
% Designated Root                   : ec:cd:6d:20:c0:ed
% Designated Cost                   : 0
% Designated Bridge                 : ec:cd:6d:20:c0:ed
% Designated Port Id                : 8393
% Top Change Ack                    : FALSE
% Config Pending                    : FALSE
% PORT Based Information & Statistics
% ----------------------------------
% Config Bpdu's xmitted             : 0
% Config Bpdu's received            : 0
% TCN Bpdu's xmitted                : 0
% TCN Bpdu's received               : 0
% Forward Trans Count               : 0
```

```
% STATUS of Port Timers
% ----------------------
% Hello Time Configured              : 2
% Hello timer                        : INACTIVE
% Hello Time Value                   : 0
% Forward Delay Timer                : INACTIVE
% Forward Delay Timer Value          : 0
% Message Age Timer                  : INACTIVE
% Message Age Timer Value            : 0
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0
% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 0
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 0
% Next State                         : Learning
% Topology Change Time               : 0
```

show spanning-tree statistics instance

Overview This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST (Multiple Spanning Tree) instance, and all switch ports associated with that MST instance.

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

Syntax

```
show spanning-tree statistics instance <instance-id>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.

Mode Privileged Exec

Example To display BPDU statistics information for MST instance 2, and all switch ports associated with that MST instance, use the command:

```
awplus# show spanning-tree statistics instance 2
```

Output Figure 17-13: Example output from **show spanning-tree statistics instance**

```
% % INST_PORT port1.0.3 Information & Statistics
% ---------------------------------------
% Config Bpdu's xmitted (port/inst)    : (0/0)
% Config Bpdu's received (port/inst)   : (0/0)
% TCN Bpdu's xmitted (port/inst)       : (0/0)
% TCN Bpdu's received (port/inst)      : (0/0)
% Message Age(port/Inst)               : (0/0)
% port1.0.3: Forward Transitions                : 0
% Next State                           : Learning
% Topology Change Time                 : 0
...
```

Related commands show spanning-tree statistics

show spanning-tree statistics instance interface

Overview This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST (Multiple Spanning Tree) instance and the specified switch port associated with that MST instance.

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

Syntax

```
show spanning-tree statistics instance <instance-id> interface
<port>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<port>	The port to display information about. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2).

Mode Privileged Exec

Example To display BPDU statistics for MST instance 2, interface port1.0.2, use the command:

```
awplus# show spanning-tree statistics instance 2 interface
port1.0.2
```

Output Figure 17-14: Example output from **show spanning-tree statistics instance interface**

```
awplus#sh spanning-tree statistics interface port1.0.2 instance 1
        Spanning Tree Enabled for Instance : 1
        ==================================
% INST_PORT port1.0.2 Information & Statistics
% ---------------------------------------
% Config Bpdu's xmitted (port/inst)    : (0/0)
% Config Bpdu's received (port/inst)   : (0/0)
% TCN Bpdu's xmitted (port/inst)       : (0/0)
% TCN Bpdu's received (port/inst)      : (0/0)
% Message Age(port/Inst)               : (0/0)
% port1.0.2: Forward Transitions       : 0
% Next State                           : Learning
% Topology Change Time                 : 0

% Other Inst/Vlan Information & Statistics
% ---------------------------------------
% Bridge Priority                     : 0
% Bridge Mac Address                  : ec:cd:6d:20:c0:ed
% Topology Change Initiator           : 5023
% Last Topology Change Occured        : Mon Oct 3 05:42:06 2016
% Topology Change                     : FALSE
% Topology Change Detected            : FALSE
% Topology Change Count               : 1
% Topology Change Last Recvd from     : 00:00:00:00:00:00
```

Related commands show spanning-tree statistics

show spanning-tree statistics interface

Overview This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified switch port, and all MST instances associated with that switch port.

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

Syntax

```
show spanning-tree statistics interface <port>
```

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. port1.0.2), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2).

Mode Privileged Exec

Example To display BPDU statistics about each MST instance for port1.0.2, use the command:

```
awplus# show spanning-tree statistics interface port1.0.2
```

Output Figure 17-15: Example output from **show spanning-tree statistics interface**

```
awplus#show spanning-tree statistics interface port1.0.2

              Port number = 906 Interface = port1.0.2
                 ================================
% BPDU Related Parameters
% ----------------------
% Port Spanning Tree                : Disable
% Spanning Tree Type                : Multiple Spanning Tree Protocol
% Current Port State                : Discarding
% Port ID                           : 838a
% Port Number                       : 38a
% Path Cost                         : 20000000
% Message Age                       : 0
% Designated Root                   : ec:cd:6d:20:c0:ed
% Designated Cost                   : 0
% Designated Bridge                 : ec:cd:6d:20:c0:ed
% Designated Port Id                : 838a
% Top Change Ack                    : FALSE
% Config Pending                    : FALSE
```

```
% PORT Based Information & Statistics
% -----------------------------------
% Config Bpdu's xmitted              : 0
% Config Bpdu's received             : 0
% TCN Bpdu's xmitted                 : 0
% TCN Bpdu's received                : 0
% Forward Trans Count                : 0

% STATUS of Port Timers
% ---------------------
% Hello Time Configured              : 2
% Hello timer                        : INACTIVE
% Hello Time Value                   : 0
% Forward Delay Timer                : INACTIVE
% Forward Delay Timer Value          : 0
% Message Age Timer                  : INACTIVE
% Message Age Timer Value            : 0
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0

% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 0
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 0
% Next State                         : Learning
% Topology Change Time               : 0
% Other Bridge information & Statistics
  -------------------------------------
% STP Multicast Address              : 01:80:c2:00:00:00
% Bridge Priority                    : 32768
% Bridge Mac Address                 : ec:cd:6d:20:c0:ed
% Bridge Hello Time                  : 2
% Bridge Forward Delay               : 15
% Topology Change Initiator          : 5023
% Last Topology Change Occured       : Mon Oct 3 05:41:20 2016
% Topology Change                    : FALSE
% Topology Change Detected           : TRUE
% Topology Change Count              : 1
% Topology Change Last Recvd from    : 00:00:00:00:00:00
```

Related commands show spanning-tree statistics

show spanning-tree vlan range-index

Overview Use this command to display information about MST (Multiple Spanning Tree) instances and the VLANs associated with them including the VLAN range-index value for the device.

Syntax

```
show spanning-tree vlan range-index
```

Mode Privileged Exec

Example To display information about MST instances and the VLANs associated with them for the device, including the VLAN range-index value, use the following command:

```
awplus# show spanning-tree vlan range-index
```

Output Figure 17-16: Example output from **show spanning-tree vlan range-index**

```
awplus#show spanning-tree vlan range-index
% MST Instance  VLAN       RangeIdx
%      1        1          1%
```

Related commands show spanning-tree statistics

spanning-tree autoedge (RSTP and MSTP)

Overview Use this command to enable the autoedge feature on the port.

The autoedge feature allows the port to automatically detect that it is an edge port. If it does not receive any BPDUs in the first three seconds after linkup, enabling, or entering RSTP or MSTP mode, it sets itself to be an edgeport and enters the forwarding state.

Use this command for RSTP or MSTP.

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

Syntax

```
spanning-tree autoedge
no spanning-tree autoedge
```

Default Disabled

Mode Interface Configuration

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# spanning-tree autoedge
```

Related commands spanning-tree edgeport (RSTP and MSTP)

spanning-tree bpdu

Overview Use this command to configure BPDU (Bridge Protocol Data Unit) discarding or forwarding, when STP is disabled on the switch. This may be needed for correct STP operation in complex networks.

There is no **no** variant for this command. Instead, apply the **discard** parameter to reset it back to the default then re-enable STP with the command spanning-tree enable.

Syntax

```
spanning-tree bpdu
{discard|forward|forward-untagged-vlan|forward-vlan}
```

Parameter	Description	
`bpdu`	A port that has BPDU filtering enabled will not transmit any BPDUs and will ignore any BPDUs received. This port type has one of the following parameters (in Global Configuration mode):	
	`discard`	Discards all ingress STP BPDU frames.
	`forward`	Forwards any ingress STP BPDU packets to all ports, regardless of any VLAN membership.
	`forward-untagged-vlan`	Forwards any ingress STP BPDU frames to all ports that are untagged members of the ingress port's native VLAN.
	`forward-vlan`	Forwards any ingress STP BPDU frames to all ports that are tagged members of the ingress port's native VLAN.

Default The discard parameter is enabled by default.

Mode Global Configuration

Usage notes This command enables the switch to forward unsupported BPDUs with an unsupported Spanning Tree Protocol, such as proprietary STP protocols with unsupported BPDUs, by forwarding BDPU (Bridge Protocol Data Unit) frames unchanged through the switch.

You must disable RSTP with the **no spanning-tree rstp enable** command before you can use this command.

When you want to revert to default behavior on the switch, issue a **spanning-tree bdpu discard** command and re-enable Spanning Tree with a **spanning-tree rstp enable** command.

Examples

To enable STP BPDU discard in Global Configuration mode with STP disabled, which discards all ingress STP BPDU frames, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree rstp enable
awplus(config)# spanning-tree bpdu discard
```

To enable STP BPDU forward in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports regardless of any VLAN membership, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree rstp enable
awplus(config)# spanning-tree bpdu forward
```

To enable STP BPDU forwarding for untagged frames in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports that are untagged members of the ingress port's native VLAN, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree rstp enable
awplus(config)# spanning-tree bpdu forward-untagged-vlan
```

To enable STP BPDU forwarding for tagged frames in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports that are tagged members of the ingress port's native VLAN, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree rstp enable
awplus(config)# spanning-tree bpdu forward-vlan
```

To reset STP BPDU back to the default `discard` parameter and re-enable RSTP on the switch, enter the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree bpdu discard
awplus(config)# spanning-tree rstp enable
```

Related commands

show spanning-tree

spanning-tree enable

spanning-tree cisco-interoperability (MSTP)

Overview Use this command to enable/disable Cisco-interoperability for MSTP.

Use this command for MSTP only.

Syntax

```
spanning-tree cisco-interoperability {enable|disable}
```

Parameter	Description
`enable`	Enable Cisco interoperability for MSTP.
`disable`	Disable Cisco interoperability for MSTP.

Default If this command is not used, Cisco interoperability is disabled.

Mode Global Configuration

Usage For compatibility with certain Cisco devices, all devices in the switched LAN running the AlliedWare Plus™ Operating System must have Cisco-interoperability enabled. When the AlliedWare Plus Operating System is interoperating with Cisco, the only criteria used to classify a region are the region name and revision level. VLAN to instance mapping is not used to classify regions when interoperating with Cisco.

Examples To enable Cisco interoperability on a Layer 2 device:

```
awplus# configure terminal
awplus(config)# spanning-tree cisco-interoperability enable
```

To disable Cisco interoperability on a Layer 2 device:

```
awplus# configure terminal
awplus(config)# spanning-tree cisco-interoperability disable
```

spanning-tree edgeport (RSTP and MSTP)

Overview Use this command to set a port as an edge-port.

Use this command for RSTP or MSTP.

This command has the same effect as the spanning-tree portfast (STP) command, but the configuration displays differently in the output of some show commands.

Use the **no** variant of this command to set a port to its default state (not an edge-port).

Syntax

```
spanning-tree edgeport
no spanning-tree edgeport
```

Default Not an edge port.

Mode Interface Configuration

Usage notes Use this command on a switch port connected to a LAN that has no other bridges attached. If a BPDU is received on the port that indicates that another bridge is connected to the LAN, then the port is no longer treated as an edge port.

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree edgeport
```

Related commands spanning-tree autoedge (RSTP and MSTP)

spanning-tree enable

Overview Use this command in Global Configuration mode to enable the specified spanning tree protocol for all switch ports. Note that this must be the spanning tree protocol that is configured on the device by the spanning-tree mode command.

Use the **no** variant of this command to disable the configured spanning tree protocol. This places all switch ports in the forwarding state.

Syntax

```
spanning-tree {mstp|rstp|stp} enable
no spanning-tree {mstp|rstp|stp} enable
```

Parameter	Description
`mstp`	Enables or disables MSTP (Multiple Spanning Tree Protocol).
`rstp`	Enables or disables RSTP (Rapid Spanning Tree Protocol).
`stp`	Enables or disables STP (Spanning Tree Protocol).

Default RSTP is enabled by default for all switch ports.

Mode Global Configuration

Usage With no configuration, spanning tree is enabled, and the spanning tree mode is set to RSTP. To change the mode, see spanning-tree mode command.

Examples To enable STP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree stp enable
```

To disable STP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
```

To enable MSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mstp enable
```

To disable MSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree mstp enable
```

To enable RSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree rstp enable
```

To disable RSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree rstp enable
```

Related commands

spanning-tree bpdu

spanning-tree mode

spanning-tree errdisable-timeout enable

Overview Use this command to enable the errdisable-timeout facility, which sets a timeout for ports that are disabled due to the BPDU guard feature.

Use this command for RSTP or MSTP.

Use the **no** variant of this command to disable the errdisable-timeout facility.

Syntax
```
spanning-tree errdisable-timeout enable
no spanning-tree errdisable-timeout enable
```

Default By default, the errdisable-timeout is disabled.

Mode Global Configuration

Usage The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port. This command associates a timer with the feature such that the port is re- enabled without manual intervention after a set interval. This interval can be configured by the user using the spanning-tree errdisable-timeout interval command.

Example
```
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout enable
```

Related commands
show spanning-tree

spanning-tree errdisable-timeout interval

spanning-tree portfast bpdu-guard

spanning-tree errdisable-timeout interval

Overview Use this command to specify the time interval after which a port is brought back up when it has been disabled by the BPDU guard feature.

Use this command for RSTP or MSTP.

Syntax

```
spanning-tree errdisable-timeout interval <10-1000000>
no spanning-tree errdisable-timeout interval
```

Parameter	Description
<10-1000000>	Specify the errdisable-timeout interval in seconds.

Default By default, the port is re-enabled after 300 seconds.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout interval 34
```

Related commands

show spanning-tree

spanning-tree errdisable-timeout enable

spanning-tree portfast bpdu-guard

spanning-tree force-version

Overview Use this command in Interface Configuration mode for a switch port interface only to force the protocol version for the switch port. Use this command for RSTP or MSTP only.

Syntax

```
spanning-tree force-version <version>
no spanning-tree force-version
```

Parameter	Description	
<version>	<0-3>	Version identifier.
	0	Forces the port to operate in STP mode.
	1	Not supported.
	2	Forces the port to operate in RSTP mode. If it receives STP BPDUs, it can automatically revert to STP mode.
	3	Forces the port to operate in MSTP mode (this option is only available if MSTP mode is configured). If it receives RSTP or STP BPDUs, it can automatically revert to RSTP or STP mode.

Default By default, no version is forced for the port. The port is in the spanning tree mode configured for the device, or a lower version if it automatically detects one.

Mode Interface Configuration mode for a switch port interface only.

Examples Set the value to enforce the spanning tree protocol (STP):

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree force-version 0
```

Set the default protocol version:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree force-version
```

Related commands show spanning-tree

spanning-tree forward-time

Overview Use this command to set the forward delay value. Use the **no** variant of this command to reset the forward delay value to the default setting of 15 seconds.

The **forward delay** sets the time (in seconds) to control how fast a port changes its spanning tree state when moving towards the forwarding state. If the mode is set to STP, the value determines how long the port stays in each of the listening and learning states which precede the forwarding state. If the mode is set to RSTP or MSTP, this value determines the maximum time taken to transition from discarding to learning and from learning to forwarding.

This value is used only when the device is acting as the root bridge. Devices not acting as the Root Bridge use a dynamic value for the **forward delay** set by the root bridge. The **forward delay**, **max-age**, and **hello time** parameters are interrelated.

Syntax

```
spanning-tree forward-time <forward-delay>
no spanning-tree forward-time
```

Parameter	Description
<forward-delay>	<4-30> The forwarding time delay in seconds.

Default The default is 15 seconds.

Mode Global Configuration

Usage notes The allowable range for forward-time is 4-30 seconds.

The **forward delay**, **max-age**, and **hello time** parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

2 x (forward delay - 1.0 seconds) >= max-age

max-age >= 2 x (hello time + 1.0 seconds)

Example

```
awplus# configure terminal
awplus(config)# spanning-tree forward-time 6
```

Related commands

show spanning-tree

spanning-tree forward-time

spanning-tree hello-time

spanning-tree mode

spanning-tree guard root

Overview Use this command in Interface Configuration mode for a switch port only to enable the Root Guard feature for the switch port. The root guard feature disables reception of superior BPDUs. You can use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to disable the root guard feature for the port.

Syntax

```
spanning-tree guard root
no spanning-tree guard root
```

Mode Interface Configuration mode for a switch port interface only.

Usage notes The Root Guard feature makes sure that the port on which it is enabled is a designated port. If the Root Guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree guard root
```

spanning-tree hello-time

Overview Use this command to set the hello-time. This sets the time in seconds between the transmission of device spanning tree configuration information when the device is the Root Bridge of the spanning tree or is trying to become the Root Bridge.

Use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to restore the default of the hello time.

Syntax

```
spanning-tree hello-time <hello-time>
no spanning-tree hello-time
```

Parameter	Description
<hello-time>	<1-10> The hello BPDU interval in seconds.

Default Default is 2 seconds.

Mode Global Configuration and Interface Configuration for switch ports.

Usage notes The allowable range of values is 1-10 seconds.

The forward delay, max-age, and hello time parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

2 x (forward delay - 1.0 seconds) >= max-age

max-age>= 2 x (hello time + 1.0 seconds)

Example

```
awplus# configure terminal
awplus(config)# spanning-tree hello-time 3
```

Related commands

spanning-tree forward-time

spanning-tree max-age

show spanning-tree

spanning-tree link-type

Overview Use this command in Interface Configuration mode for a switch port interface only to enable or disable point-to-point or shared link types on the switch port.

Use this command for RSTP or MSTP only.

Use the **no** variant of this command to return the port to the default link type.

Syntax

```
spanning-tree link-type {point-to-point|shared}
no spanning-tree link-type
```

Parameter	Description
`shared`	Disable rapid transition.
`point-to-point`	Enable rapid transition.

Default The default link type is point-to-point.

Mode Interface Configuration mode for a switch port interface only.

Usage notes You may want to set link type to shared if the port is connected to a hub with multiple devices connected to it.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree link-type point-to-point
```

spanning-tree max-age

Overview Use this command to set the max-age. This sets the maximum age, in seconds, that dynamic spanning tree configuration information is stored in the device before it is discarded.

Use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to restore the default of max-age.

Syntax

```
spanning-tree max-age <max-age>
no spanning-tree max-age
```

Parameter	Description
<max-age>	<6-40> The maximum time, in seconds.

Default The default of spanning-tree max-age is 20 seconds.

Mode Global Configuration

Usage Max-age is the maximum time in seconds for which a message is considered valid.

Configure this value sufficiently high, so that a frame generated by the root bridge can be propagated to the leaf nodes without exceeding the max-age.

The **forward delay**, **max-age**, and **hello time** parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

2 x (forward delay - 1.0 seconds) >= max-age

max-age >= 2 x (hello time + 1.0 seconds)

Example

```
awplus# configure terminal
awplus(config)# spanning-tree max-age 12
```

Related commands

show spanning-tree

spanning-tree forward-time

spanning-tree hello-time

spanning-tree max-hops (MSTP)

Overview Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST region.

Use the **no** variant of this command to restore the default.

Use this command for MSTP only.

Syntax

```
spanning-tree max-hops <hop-count>
no spanning-tree max-hops <hop-count>
```

Parameter	Description
<hop-count>	Specify the maximum hops the BPDU will be valid for in the range <1-40>.

Default The default max-hops in a MST region is 20.

Mode Global Configuration

Usage Specifying the max hops for a BPDU prevents the messages from looping indefinitely in the network. The hop count is decremented by each receiving port. When a device receives an MST BPDU that has a hop count of zero, it discards the BPDU.

Examples

```
awplus# configure terminal
awplus(config)# spanning-tree max-hops 25
awplus# configure terminal
awplus(config)# no spanning-tree max-hops
```

spanning-tree mode

Overview Use this command to change the spanning tree protocol mode on the device. The spanning tree protocol mode on the device can be configured to either STP, RSTP or MSTP.

Syntax

```
spanning-tree mode {stp|rstp|mstp}
```

Default The default spanning tree protocol mode on the device is RSTP.

Mode Global Configuration

Usage With no configuration, the device will have spanning tree enabled, and the spanning tree mode will be set to RSTP. Use this command to change the spanning tree protocol mode on the device. MSTP is VLAN aware, but RSTP and STP are not VLAN aware. To enable or disable spanning tree operation, see the spanning-tree enable command.

Examples To change the spanning tree mode from the default of RSTP to MSTP, use the following commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
```

Related commands spanning-tree enable

spanning-tree mst configuration

Overview Use this command to enter the MST Configuration mode to configure the Multiple Spanning-Tree Protocol.

Syntax

```
spanning-tree mst configuration
```

Mode Global Configuration

Examples The following example uses this command to enter MST Configuration mode. Note the change in the command prompt.

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)#
```

spanning-tree mst instance

Overview Use this command to assign a Multiple Spanning Tree instance (MSTI) to a switch port or channel group.

Note that ports are automatically configured to send and receive spanning-tree information for the associated MSTI when VLANs are assigned to MSTIs using the instance vlan (MSTP) command.

Use the **no** variant of this command in Interface Configuration mode to remove the MSTI from the specified switch port or channel group.

Syntax

```
spanning-tree mst instance <instance-id>
no spanning-tree mst instance <instance-id>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15. The MST instance must have already been created using the instance vlan (MSTP) command.

Default A port automatically becomes a member of an MSTI when it is assigned to a VLAN.

Mode Interface Configuration mode for a switch port or channel group.

Usage notes You can disable automatic configuration of member ports of a VLAN to an associated MSTI by using a **no spanning-tree mst instance** command to remove the member port from the MSTI. Use the **spanning-tree mst instance** command to add a VLAN member port back to the MSTI.

Examples To assign instance 3 to a switch port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3
```

To remove instance 3 from a switch port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
```

Related commands

instance vlan (MSTP)

spanning-tree mst instance path-cost

spanning-tree mst instance priority

spanning-tree mst instance restricted-role

spanning-tree mst instance restricted-tcn

spanning-tree mst instance path-cost

Overview Use this command to set the cost of a path associated with a switch port, for the specified MSTI.

This specifies the switch port's contribution to the cost of a path to the MSTI regional root via that port. This applies when the port is the root port for the MSTI.

Use the **no** variant of this command to restore the default cost value of the path.

Syntax

```
spanning-tree mst instance <instance-id> path-cost <path-cost>
no spanning-tree mst instance <instance-id> path-cost
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<path-cost>	Specify the cost of path in the range of <1-200000000>, where a lower path-cost indicates a greater likelihood of the specific interface becoming a root.

Default The default path cost values and the range of recommended path cost values depend on the port speed, as shown in the following table from the IEEE 802.1q-2003 standard.

Port speed	Default path cost	Recommended path cost range
Less than 100 Kb/s	200,000,000	20,000,000-200,000,000
1Mbps	20,000,000	2,000,000-20,000,000
10Mbps	2,000,000	200,000-2,000,000
100 Mbps	200,000	20,000-200,000
1 Gbps	20,000	2,000-20,000
10 Gbps	2,000	200-2,000
100 Gbps	200	20-200
1Tbps	20	2-200
10 Tbps	2	2-20

Mode Interface Configuration mode for a switch port interface only.

Usage notes Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the spanning-tree mst instance command.

Examples To set a path cost of 1000 on instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 path-cost 1000
```

To return the path cost to its default value on instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3 path-cost
```

Related commands

instance vlan (MSTP)

spanning-tree mst instance

spanning-tree mst instance priority

spanning-tree mst instance restricted-role

spanning-tree mst instance restricted-tcn

spanning-tree mst instance priority

Overview Use this command in Interface Configuration mode for a switch port interface only to set the port priority for an MST instance (MSTI).

Use the **no** variant of this command to restore the default priority value (128).

Syntax

```
spanning-tree mst instance <instance-id> priority <priority>
no spanning-tree mst instance <instance-id> [priority]
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<priority>	This must be a multiple of 16 and within the range <0-240>. A lower priority indicates greater likelihood of the port becoming the root port.

Default The default is 128.

Mode Interface Configuration mode for a switch port interface.

Usage notes This command sets the value of the priority field contained in the port identifier. The MST algorithm uses the port priority when determining the root port for the switch in the MSTI. The port with the lowest value has the highest priority, so it will be chosen as root port over a port that is equivalent in all other aspects but with a higher priority value.

Examples To set the priority to 112 on instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 priority 112
```

To return the priority to its default value of 128 on instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3 priority
```

Related commands

instance vlan (MSTP)

spanning-tree priority (port priority)

spanning-tree mst instance

spanning-tree mst instance path-cost

spanning-tree mst instance restricted-role

spanning-tree mst instance restricted-tcn

spanning-tree mst instance restricted-role

Overview Use this command in Interface Configuration mode for a switch port interface only to enable the restricted role for an MSTI (Multiple Spanning Tree Instance) on a switch port. Configuring the restricted role for an MSTI on a switch port prevents the switch port from becoming the root port in a spanning tree topology.

Use the **no** variant of this command to disable the restricted role for an MSTI on a switch port. Removing the restricted role for an MSTI on a switch port allows the switch port to become the root port in a spanning tree topology.

Syntax

```
spanning-tree mst instance <instance-id> restricted-role
no spanning-tree mst instance <instance-id> restricted-role
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15. The MST instance must have already been created using the instance vlan (MSTP) command.

Default The restricted role for an MSTI instance on a switch port is disabled by default.

Mode Interface Configuration mode for a switch port interface only.

Usage notes The root port is the port providing the best path from the bridge to the root bridge. Use this command to disable a port from becoming a root port. Use the **no** variant of this command to enable a port to become a root port. See the STP Feature Overview and Configuration Guide for root port information.

Examples To prevent a switch port from becoming the root port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 restricted-role
```

To stop preventing the switch port from becoming the root port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
restricted-role
```

Related commands

instance vlan (MSTP)

spanning-tree priority (port priority)

spanning-tree mst instance

spanning-tree mst instance path-cost

spanning-tree mst instance restricted-tcn

spanning-tree mst instance restricted-tcn

Overview Use this command to prevent a switch port from propagating received topology change notifications and topology changes to other switch ports. This is named restricted TCN (Topology Change Notification). A TCN is a simple Bridge Protocol Data Unit (BPDU) that a bridge sends out to its root port to signal a topology change.

Use the **no** variant of this command to stop preventing the switch port from propagating received topology change notifications and topology changes to other switch ports for the specified MSTI (Multiple Spanning Tree Instance).

The restricted TCN setting applies only to the specified MSTI (Multiple Spanning Tree Instance).

Syntax

```
spanning-tree mst instance <instance-id> restricted-tcn
no spanning-tree mst instance <instance-id> restricted-tcn
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15. The MST instance must have already been created using the instance vlan (MSTP) command.

Default Disabled. By default, switch ports propagate TCNs.

Mode Interface Configuration mode for a switch port interface only.

Examples To prevent a switch port from propagating received topology change notifications and topology changes to other switch ports, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 restricted-tcn
```

To stop preventing a switch port from propagating received topology change notifications and topology changes to other switch ports, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
restricted-tcn
```

Related commands

instance vlan (MSTP)

spanning-tree priority (port priority)

spanning-tree mst instance

spanning-tree mst instance path-cost

spanning-tree mst instance restricted-role

spanning-tree path-cost

Overview Use this command in Interface Configuration mode for a switch port interface only to set the cost of a path for the specified port. This value then combines with others along the path to the root bridge in order to determine the total cost path value from the particular port, to the root bridge. The lower the numeric value, the higher the priority of the path. This applies when the port is the root port.

Use this command for RSTP, STP or MSTP. When MSTP mode is configured, this will apply to the port's path cost for the CIST.

Syntax

```
spanning-tree path-cost <pathcost>
no spanning-tree path-cost
```

Parameter	Description
<pathcost>	<1-200000000> The cost to be assigned to the port.

Default The default path cost values and the range of recommended path cost values depend on the port speed, as shown in the following table from the IEEE 802.1q-2003 and IEEE 802.1d-2004 standards.

Port speed	Default path cost	Recommended path cost range
Less than 100 Kb/s	200,000,000	20,000,000-200,000,000
1Mbps	20,000,000	2,000,000-20,000,000
10Mbps	2,000,000	200,000-2,000,000
100 Mbps	200,000	20,000-200,000
1 Gbps	20,000	2,000-20,000
10 Gbps	2,000	200-2, 000
100 Gbps	200	20-200
1Tbps	20	2-200
10 Tbps	2	2-20

Mode Interface Configuration mode for switch port interface only.

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree path-cost 123
```

spanning-tree portfast (STP)

Overview Use this command in Interface Configuration mode for a switch port interface only to set a port as an edge-port. The portfast feature enables a port to rapidly move to the forwarding state, without having first to pass through the intermediate spanning tree states. This command has the same effect as the spanning-tree edgeport (RSTP and MSTP) command, but the configuration displays differently in the output of some show commands.

NOTE: *You can run either of two additional parameters with this command. To simplify the syntax these are documented as separate commands. See the following additional portfast commands:*

- spanning-tree portfast bpdu-filter command
- spanning-tree portfast bpdu-guard command.

You can obtain the same effect by running the spanning-tree edgeport (RSTP and MSTP) command. However, the configuration output may display differently in some show commands.

Use the **no** variant of this command to set a port to its default state (not an edge-port).

Syntax

```
spanning-tree portfast
no spanning-tree portfast
```

Default Not an edge port.

Mode Interface Configuration mode for a switch port interface only.

Usage notes Portfast makes a port move from a blocking state to a forwarding state, bypassing both listening and learning states. The portfast feature is meant to be used for ports connected to end-user devices. Enabling portfast on ports that are connected to a workstation or server allows devices to connect to the network without waiting for spanning-tree to converge.

For example, you may need hosts to receive a DHCP address quickly and waiting for STP to converge would cause the DHCP request to time out. Ensure you do not use portfast on any ports connected to another device to avoid creating a spanning-tree loop on the network.

Use this command on a switch port that connects to a LAN with no other bridges attached. An edge port should never receive BPDUs. Therefore if an edge port receives a BPDU, the portfast feature takes one of three actions.

- Cease to act as an edge port and pass BPDUs as a member of a spanning tree network (spanning-tree portfast (STP) command disabled).
- Filter out the BPDUs and pass only the data and continue to act as a edge port (spanning-tree portfast bpdu-filter command enabled).
- Block the port to all BPDUs and data (spanning-tree portfast bpdu-guard command enabled).

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree portfast
```

Related commands

spanning-tree edgeport (RSTP and MSTP)

show spanning-tree

spanning-tree portfast bpdu-filter

spanning-tree portfast bpdu-guard

spanning-tree portfast bpdu-filter

Overview This command sets the bpdu-filter feature and applies a filter to any BPDUs (Bridge Protocol Data Units) received. Enabling this feature ensures that configured ports will not transmit any BPDUs and will ignore (filter out) any BPDUs received. BPDU Filter is not enabled on a port by default.

Using the **no** variant of this command to turn off the bpdu-filter, but retain the port's status as an enabled port. If the port then receives a BPDU it will change its role from an **edge-port** to a **non edge-port**.

Syntax (Global Configuration)

```
spanning-tree portfast bpdu-filter
no spanning-tree portfast bpdu-filter
```

Syntax (Interface Configuration)

```
spanning-tree portfast bpdu-filter
{default|disable|enable}
no spanning-tree portfast bpdu-filter
```

Parameter	Description	
`bpdu-filter`	A port that has bpdu-filter enabled will not transmit any BPDUs and will ignore any BPDUs received. This port type has one of the following parameters (in Interface Configuration mode):	
	`default`	Takes the setting that has been configured for the whole device, i.e. the setting made from the Global configuration mode.
	`disable`	Turns off BPDU filter.
	`enable`	Turns on BPDU filter.

Default BPDU Filter is not enabled on any ports by default.

Mode Global Configuration and Interface Configuration

Usage notes This command filters the BPDUs and passes only data to continue to act as an edge port. Using this command in Global Configuration mode applies the portfast bpdu-filter feature to all ports on the device. Using it in Interface mode applies the feature to a specific port, or range of ports.The command will operate in both RSTP and MSTP networks.

Use the show spanning-tree command to display status of the bpdu-filter parameter for the switch ports.

Example To enable STP BPDU filtering in Global Configuration mode, enter the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-filter
```

To enable STP BPDU filtering in Interface Configuration mode, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree portfast bpdu-filter enable
```

Related commands

spanning-tree edgeport (RSTP and MSTP)

show spanning-tree

spanning-tree portfast (STP)

spanning-tree portfast bpdu-guard

spanning-tree portfast bpdu-guard

Overview

This command applies a BPDU (Bridge Protocol Data Unit) guard to the port. A port with the bpdu-guard feature enabled will block all traffic (BPDUs and user data), if it starts receiving BPDUs.

Use this command in Global Configuration mode to apply BPDU guard to all ports on the device. Use this command in Interface mode for an individual interface or a range of interfaces specified. BPDU Guard is not enabled on a port by default.

Use the **no** variant of this command to disable the BPDU Guard feature on a device in Global Configuration mode or to disable the BPDU Guard feature on a port in Interface mode.

Syntax (Global Configuration)

```
spanning-tree portfast bpdu-guard
no spanning-tree portfast bpdu-guard
```

Syntax (Interface Configuration)

```
spanning-tree portfast bpdu-guard
{default|disable|enable}
no spanning-tree portfast bpdu-guard
```

Parameter	Description	
`bpdu-guard`	A port that has bpdu-guard turned on will enter the STP blocking state if it receives a BPDU. This port type has one of the following parameters (in Interface Configuration mode):	
	`default`	Takes the setting that has been configured for the whole device, i.e. the setting made from the Global configuration mode.
	`disable`	Turns off BPDU guard.
	`enable`	Turns on BPDU guard and will also set the port as an edge port.

Default

BPDU Guard is not enabled on any ports by default.

Mode

Global Configuration or Interface Configuration

Usage notes

This command blocks the port(s) to all devices and data when enabled. BPDU Guard is a port-security feature that changes how a portfast-enabled port behaves if it receives a BPDU. When **bpdu-guard** is set, then the port shuts down if it receives a BPDU. It does not process the BPDU as it is considered suspicious. When **bpdu-guard** is not set, then the port will negotiate spanning-tree with the device sending the BPDUs. By default, bpdu- guard is not enabled on a port.

You can configure a port disabled by the bpdu-guard to re-enable itself after a specific time interval. This interval is set with the spanning-tree errdisable-timeout interval command. If you do not use the **errdisable-timeout** feature, then you will need to manually re-enable the port by using the **no shutdown** command.

Use the show spanning-tree command to display the device and port configurations for the BPDU Guard feature. It shows both the administratively configured and currently running values of bpdu-guard.

Example To enable STP BPDU guard in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-guard
```

To enable STP BPDU guard in Interface Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree portfast bpdu-guard enable
```

Related commands

spanning-tree edgeport (RSTP and MSTP)

show spanning-tree

spanning-tree portfast (STP)

spanning-tree portfast bpdu-filter

spanning-tree priority (bridge priority)

Overview Use this command to set the bridge priority for the device. A lower priority value indicates a greater likelihood of the device becoming the root bridge.

Use this command for RSTP, STP or MSTP. When MSTP mode is configured, this will apply to the CIST.

Use the **no** variant of this command to reset it to the default.

Syntax

```
spanning-tree priority <priority>
no spanning-tree priority
```

Parameter	Description
<priority>	<0-61440> The bridge priority, which will be rounded to a multiple of 4096.

Default The default priority is 32678.

Mode Global Configuration

Usage To force a particular device to become the root bridge use a lower value than other devices in the spanning tree.

Example

```
awplus# configure terminal
awplus(config)# spanning-tree priority 4096
```

Related commands

spanning-tree mst instance priority

show spanning-tree

spanning-tree priority (port priority)

Overview Use this command in Interface Configuration mode for a switch port interface only to set the port priority for port. A lower priority value indicates a greater likelihood of the port becoming part of the active topology.

Use this command for RSTP, STP, or MSTP. When the device is in MSTP mode, this will apply to the CIST.

Use the **no** variant of this command to reset it to the default.

Syntax

```
spanning-tree priority <priority>
no spanning-tree priority
```

Parameter	Description
<priority>	<0-240>, in increments of 16. The port priority, which will be rounded down to a multiple of 16.

Default The default priority is 128.

Mode Interface Configuration mode for a switch port interface only.

Usage notes To force a port to be part of the active topology (for instance, become the root port or a designated port) use a lower value than other ports on the device. (This behavior is subject to network topology, and more significant factors, such as bridge ID.)

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree priority 16
```

Related commands

spanning-tree mst instance priority

spanning-tree priority (bridge priority)

show spanning-tree

spanning-tree restricted-role

Overview Use this command in Interface Configuration mode for a switch port interface only to restrict the port from becoming a root port.

Use the **no** variant of this command to disable the restricted role functionality.

Syntax
```
spanning-tree restricted-role
no spanning-tree restricted-role
```

Default The restricted role is disabled.

Mode Interface Configuration mode for a switch port interface only.

Example
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree restricted-role
```

spanning-tree restricted-tcn

Overview Use this command in Interface Configuration mode for a switch port interface only to prevent TCN (Topology Change Notification) BPDUs (Bridge Protocol Data Units) from being sent on a port. If this command is enabled, after a topology change a bridge is prevented from sending a TCN to its designated bridge.

Use the **no** variant of this command to disable the restricted TCN functionality.

Syntax
```
spanning-tree restricted-tcn
no spanning-tree restricted-tcn
```

Default The restricted TCN is disabled.

Mode Interface Configuration mode for a switch port interface only.

Example
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree restricted-tcn
```

spanning-tree transmit-holdcount

Overview Use this command to set the maximum number of BPDU transmissions that are held back.

Use the **no** variant of this command to restore the default transmit hold-count value.

Syntax

```
spanning-tree transmit-holdcount
no spanning-tree transmit-holdcount
```

Default Transmit hold-count default is 3.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# spanning-tree transmit-holdcount
```

undebug mstp

Overview This command applies the functionality of the no debug mstp (RSTP and STP) command.

18 Unidirectional Link Detection (UDLD) Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure the Unidirectional Link Detection (UDLD) protocol.

UDLD is a data link protocol which monitors network cables and detects broken bidirectional links. It complements the spanning tree protocol (STP), which is used to eliminate Layer 2 loops.

A license is required to use this feature. Please contact your authorized Allied Telesis representative for more information.

Command List

- "debug udld" on page 746
- "show debugging udld" on page 747
- "show udld" on page 748
- "show udld neighbors" on page 749
- "show udld port" on page 750
- "udld aggressive-mode" on page 751
- "udld enable" on page 752
- "udld port" on page 753
- "udld port aggressive-mode" on page 754
- "udld port disable" on page 755
- "udld reset" on page 756
- "udld time disable-period" on page 757
- "udld time message-interval" on page 758
- "undebug udld" on page 759

debug udld

Overview Use this command to enable UDLD debugging.

Use the **no** variant of this command to disable UDLD debugging.

Syntax

```
debug udld [info|pkt|state|nsm|all]
no debug udld [info|pkt|state|nsm|all]
```

Parameter	Description
`info`	Enable or disable general UDLD debugging information.
`pkt`	Enable or disable debugging of UDLD packets.
`state`	Enable or disable UDLD state transition debugging.
`nsm`	Enable or disable UDLD Network Service Module (NSM) debugging information.
`all`	Enable or disable the all UDLD debugging.

Default Debugging is disabled for **all** by default.

Mode Global Configuration

Privileged Exec

Example To enable UDLD packet debugging, use the commands:

```
awplus# configure terminal
awplus(config)# debug udld pkt
```

Related commands show debugging udld

undebug udld

show debugging udld

Overview Use this command to show which UDLD debugging options are set.

Syntax

```
show debugging udld
```

Mode Privileged Exec

Example To show which UDLD debugging options are set, use the command:

```
awplus# show debugging udld
```

Output Figure 18-1: Example output from **show debugging udld**

```
awplus# show debugging udld
UDLD debugging status:
 Info debugging  : off
 Packet debugging: off
 State debugging : on
 NSM debugging   : off
```

Related commands debug udld

show udld

Overview Use this command to display global UDLD status and configuration settings.

Syntax

```
show udld
```

Mode Privileged Exec

Example To show global UDLD information, use the command:

```
awplus# show udld
```

Output Figure 18-2: Example output from **show udld**

```
awplus#show udld
Status          : Enabled
Mode            : Normal
Message-Interval: 7 seconds
Timeout-Interval: 5 seconds
Disable-Period  : 15 seconds

[Fiber-Ports]
Port         Status   Mode       Directional-State
------------ -------- ---------- -----------------
port1.0.1    Enabled  Aggressive Bidirectional
port1.0.2    Disabled Normal     -
```

Related commands

udld port

udld port disable

udld enable

show udld neighbors

Overview Use this command to display UDLD neighbor status.

Syntax

```
show udld neighbors [<interface-name>] [detail]
```

Parameter	Description
<interface-name>	Show UDLD neighbor information for a specified interface.
`detail`	This option provides a greater level of detail.

Mode Privileged Exec

Example To show UDLD information for all neighbors, use the command:

```
awplus# show udld neighbors
```

To show detailed UDLD neighbor information for port1.0.1, use the command:

```
awplus# show udld neighbours port1.0.1 detail
```

Output Figure 18-3: Example output from **show udld neighbors**

```
awplus#show udld neighbors
Port         Device-ID    Port-ID      Device-Name   Neighbor-State
------------ ------------ ------------ ------------- --------------
port1.0.1    0000F4272DA2 port2.0.1    X930          Bidirectional
port1.0.2    0000F5572632 port1.0.15   X610          Bidirectional
```

Figure 18-4: Example output from **show udld neighbor port1.0.1 detail**

```
awplus# show udld neighbor port1.0.1 detail
[port1.0.1]
Device-ID         : 0000F4272DA2
Port-ID           : port2.0.1
Device-Name       : X930
Operational-State: Bidirectional
Expiration-time   : 35 seconds
Message-Interval : 15 seconds
Timeout-Interval : 5 seconds

Neighbors in Echo:
 Device-ID    Port-ID
 ------------ ------------
 0000F4272DA2 port2.0.1
 0000F5572632 port1.0.15
```

Related commands

udld port

udld port disable

udld enable

show udld port

Overview Use this command to display UDLD port status and configuration settings.

Syntax

```
show udld port [<interface-name>] [detail]
```

Parameter	Description
<interface-name>	Show UDLD information for a specified interface.
`detail`	This option provides a greater level of detail.

Mode Privileged Exec

Example To show UDLD information for all ports, use the command:

```
awplus# show udld port
```

To show detailed UDLD information for port1.0.1, use the command:

```
awplus# show udld port port1.0.1 detail
```

Output Figure 18-5: Example output from **show udld port**

```
awplus#show udld port
Port         Status   Mode       Directional-State
------------ -------- ---------- -----------------
port1.0.1    Enabled  Aggressive Bidirectional
port1.0.2    Disabled Normal     -
```

Figure 18-6: Example output from **show udld port port1.0.1 detail**

```
awplus#show udld port port1.0.1 detail
[port1.0.1]
Status           : Enabled
Mode             : Aggressive
Directional-State: Bidirectional
Operational-State: Advertisement - single neighbor detected

Neighbors:
 Device-ID    Port-ID      Device-Name      Directional-State
 ------------ ------------ ---------------- -----------------
 0000F4272DA2 port2.0.1    awplus           Bidirectional
```

Related commands

udld port

udld port disable

udld enable

udld aggressive-mode

Overview Use this command to set UDLD to aggressive mode on all interfaces.

In **normal mode**, when the UDLD information times out:

- No action is taken by UDLD.
- The UDLD port state is set to undetermined.
- The port behaves according to its STP state.

In **aggressive mode**, when the UDLD information times out:

- UDLD tries to re-establish the state of the port.
- If not successful, after 8 retries, the port is disabled.

Use the **no** variant of this command to disable aggressive mode on all interfaces.

Syntax

```
udld aggressive-mode
no udld aggressive-mode
```

Default Aggressive mode is disabled by default.

Mode Global Configuration

Example To enable aggressive mode on interfaces, use the commands:

```
awplus# configure terminal
awplus(config)# udld aggressive-mode
```

To disable aggressive mode, use the commands:

```
awplus# configure terminal
awplus(config)# no udld aggressive-mode
```

Related commands udld port aggressive-mode

show udld

udld enable

Overview Use this command to enable UDLD on all of a device's fiber-optic ports. It has no effect on copper ports. Use the udld port command to enable UDLD on copper ports.

Use the **no** variant of this command to disable the UDLD feature on all of a device's fiber interfaces.

Syntax

```
udld enable
no udld enable
```

Default UDLD is disabled by default.

Mode Global Configuration

Example To enable the UDLD feature on all fiber interfaces, use the command:

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

Related commands

show udld

show udld neighbors

udld aggressive-mode

udld port

udld port disable

udld reset

udld time disable-period

udld time message-interval

udld port

Overview Use this command to enable UDLD on an interface.This command enables UDLD on both copper and fiber ports.

Use the **no** variant of this command to disable UDLD on an interface.

Syntax

```
udld port
no udld port
```

Default UDLD is disabled on an interface by default.

Mode Interface Configuration

Usage notes

- This command always enables the UDLD feature on a port.
- The udld port disable command overwrites this command and disables UDLD on an interface.
- If UDLD has been set globally, using the udld enable command, then AlliedWare Plus ignores the **no udld port** command on a fiber interface.

Example To enable UDLD on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# udld port
```

To disable UDLD on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no udld port
```

Related commands

show udld port

show udld neighbors

udld enable

udld port disable

udld reset

udld time disable-period

udld time message-interval

udld port aggressive-mode

Overview Use this command to enable UDLD aggressive mode on an interface.

In **normal mode**, when the UDLD information times out:

- No action is taken by UDLD.
- The UDLD port state is set to undetermined.
- The port behaves according to its STP state.

In **aggressive mode**, when the UDLD information times out:

- UDLD tries to re-establish the state of the port.
- If not successful, after 8 retries, the port is disabled.

Use the **no** variant of this command to disable aggressive mode on an interface.

Syntax

```
udld port aggressive-mode
no udld port aggressive-mode
```

Default Aggressive mode is disabled on an interface by default.

Mode Interface Configuration

Example To change the UDLD mode to aggressive on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# udld port aggressive-mode
```

To disable aggressive mode on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no port aggressive-mode
```

Related commands udld aggressive-mode

show udld port

udld port disable

Overview Use this command to disable UDLD on an interface. This command disables UDLD on both copper and fiber ports

Use the **no** variant of this command to allow UDLD on a fiber port.

Syntax

```
udld port disable
no udld port disable
```

Default UDLD disable is not set by default.

Usage notes

- This command always disables the UDLD feature on a port.
- The udld port command overwrites this command and enables UDLD on an interface.
- If UDLD has been set globally, using the udld enable command, then AlliedWare Plus ignores the **no udld port** command on a fiber interface.

Mode Interface Configuration

Example To disable UDLD on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# udld port disable
```

To enable UDLD on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no udld port disable
```

Related commands

udld enable

udld port

show udld port

udld reset

Overview Use this command to reset the status of any interface disabled by UDLD.

Syntax

```
udld reset
```

Mode Global Configuration

Example To reset an interface that has been disabled by UDLD, use the commands:

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

Output Figure 18-7: Example output from **udld reset**, when 2 ports are disabled

```
awplus#udld reset
 2 ports disabled by udld reset
```

Figure 18-8: Example output from **udld reset**, when no ports are disabled

```
awplus#udld reset
 No ports are disabled by udld reset
```

Related commands show udld

udld enable

udld time disable-period

Overview Use this command to set the UDLD disable period on all interfaces. The disable period is the time (in seconds) that a port is marked disabled before UDLD attempts to recheck it.

Manually reset the UDLD status of a port using the udld reset command.

Use the **no** variant of this command to reset the disable period to infinite.

Syntax

```
udld time disable-period <seconds>
no udld time disable-period
```

Parameter	Description
<seconds>	30-86400 Specify the disable period in seconds.

Default The default time disable period is infinite.

Mode Global Configuration

Example To change the UDLD disable period to 60 sec on all interfaces, use the commands:

```
awplus# configure terminal
awplus(config)# udld time disable-period 60
```

To reset the disable period to infinite, use the commands:

```
awplus# configure terminal
awplus(config)# no udld time disable-period
```

Related commands

udld enable

udld port

show udld

udld time message-interval

Overview Use this command to set the UDLD message send interval on all interfaces.

This is the time, in seconds, between UDLD probe messages.

Use the **no** variant of this command to reset the message send interval to 15 seconds.

Syntax

```
udld time message-interval <seconds>
no udld time message-interval
```

Parameter	Description
<seconds>	7-90 Specify the message send interval in seconds.

Default The default message send interval is 15 seconds.

Mode Global Configuration

Example To change UDLD message sending interval to 30 sec on all interfaces, use the commands:

```
awplus# configure terminal
awplus(config)# udld time message-interval 30
```

To reset the message sending interval to 15 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no udld time message-interval
```

Related commands

udld enable

udld port

show udld

undebug udld

Overview This command applies the functionality of the **no** debug udld command.

19 Link Aggregation Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure a static channel group (static aggregator) and dynamic channel group (LACP channel group, etherchannel or LACP aggregator). Link aggregation is also sometimes referred to as channeling.

NOTE: *AlliedWare Plus™ supports IEEE 802.3ad link aggregation and uses the Link Aggregation Control Protocol (LACP). LACP does not interoperate with devices that use Port Aggregation Protocol (PAgP).*

Link aggregation does not necessarily achieve exact load balancing across the links. The load sharing algorithm is designed to ensure that any given data flow always goes down the same link. It also aims to spread data flows across the links as evenly as possible.

For example, for a 2 Gbps LAG that is a combination of two 1 Gbps ports, any one flow of traffic can only ever reach a maximum throughput of 1 Gbps. However, the hashing algorithm should spread the flows across the links so that when many flows are operating, the full 2 Gbps can be utilized.

For information about load balancing see the platform load-balancing command.

For a description of static and dynamic link aggregation (LACP), and configuration examples, see the Link Aggregation Feature Overview and Configuration Guide.

Command List

- "channel-group" on page 762
- "clear lacp counters" on page 764
- "debug lacp" on page 765
- "lacp global-passive-mode enable" on page 766
- "lacp port-priority" on page 767
- "lacp system-priority" on page 768
- "lacp timeout" on page 769
- "platform load-balancing" on page 771

- "show debugging lacp" on page 772
- "show diagnostic channel-group" on page 773
- "show etherchannel" on page 775
- "show etherchannel detail" on page 776
- "show etherchannel summary" on page 777
- "show lacp sys-id" on page 778
- "show lacp-counter" on page 779
- "show port etherchannel" on page 780
- "show static-channel-group" on page 781
- "static-channel-group" on page 782
- "undebug lacp" on page 784

channel-group

Overview Use this command to create a dynamic channel group, or to add a port to an existing dynamic channel group.

You can create up to 128 channel groups, in any combination of static and dynamic (LACP) groups. This means you can create up to 128 dynamic channel groups, if you have no static channel groups.

Use the **no** variant of this command to turn off link aggregation on the device port. You will be returned to Global Configuration mode from Interface Configuration mode.

Syntax

```
channel-group <dynamic-channel-group-number> mode
{active|passive}
```

```
no channel-group
```

Parameter	Description
<dynamic-channel-group-number>	<1-248> Dynamic channel group number for an LACP link. You can create up to 128 dynamic channel groups, numbered in the range 1-248.
`active`	Enables initiation of LACP negotiation on a port. The port will transmit LACP dialogue messages whether or not it receives them from the partner device.
`passive`	Disables initiation of LACP negotiation on a port. The port will only transmit LACP dialogue messages if the partner device is transmitting them, i.e., the partner is in the active mode.

Mode Interface Configuration

Usage notes All the device ports in a channel-group must belong to the same VLANs, have the same tagging status, and can only be operated on as a group. All device ports within a channel group must have the same port speed and be in full duplex mode.

Once the LACP channel group has been created, it is treated as a device port. You can specify it in other commands. If you are specifying it in:

- an LACP command, then use the channel-group number on its own. For example, use the command **show etherchannel 2** to show details about channel group 2.
- a non-LACP command, then use **po** followed by the channel-group number. For example, use the command **show interface po2** to show details about channel group 2's interface.

For more information about LACP, see the Link Aggregation Feature Overview and Configuration Guide which is available on our website at alliedtelesis.com.

Examples

To add device port1.0.2 to a newly created LACP channel group 2, in active mode, use the commands below:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# channel-group 2 mode active
```

To remove device port1.0.2 from any created LACP channel groups, use the command below:

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

To reference channel group 2 as an interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface po2
awplus(config-if)#
```

Related commands

show etherchannel

show etherchannel detail

show etherchannel summary

show port etherchannel

Command changes

Version 5.4.9-0.1: Ability added to create up to 128 groups as any combination of static and dynamic channel groups. Also, numbering changed to 1-248.

clear lacp counters

Overview Use this command to clear all counters of all present LACP aggregators (channel groups) or a given LACP aggregator.

Syntax

```
clear lacp [<1-248>] counters
```

Parameter	Description
<1-248>	Channel-group number.

Mode Privileged Exec

Example

```
awplus# clear lacp 2 counters
```

debug lacp

Overview Use this command to enable all LACP troubleshooting functions.

Use the **no** variant of this command to disable this function.

Syntax

```
debug lacp {all|cli|event|ha|packet|sync|timer[detail]}
no debug lacp {all|cli|event|ha|packet|sync|timer[detail]}
```

Parameter	Description
`all`	Turn on all debugging for LACP.
`cli`	Specifies debugging for CLI messages. Echoes commands to the console.
`event`	Specifies debugging for LACP events. Echoes events to the console.
`ha`	Specifies debugging for HA (High Availability) events. Echoes High Availability events to the console.
`packet`	Specifies debugging for LACP packets. Echoes packet contents to the console.
`sync`	Specified debugging for LACP synchronization. Echoes synchronization to the console.
`timer`	Specifies debugging for LACP timer. Echoes timer expiry to the console.
`detail`	Optional parameter for LACP timer-detail. Echoes timer start/stop details to the console.

Mode Privileged Exec and Global Configuration

Examples

```
awplus# debug lacp timer detail
awplus# debug lacp all
```

Related commands show debugging lacp

undebug lacp

lacp global-passive-mode enable

Overview Use this command to enable LACP channel-groups to dynamically self-configure when they are connected to another device that has LACP channel-groups configured with Active Mode.

Syntax

```
lacp global-passive-mode enable
no lacp global-passive-mode enable
```

Default Enabled

Mode Global Configuration

Usage notes Do not mix LACP configurations (manual and dynamic). When LACP global passive mode is turned on (by using the **lacp global-passive-mode enable** command), we do not recommend using a mixed configuration in a LACP channel-group; i.e. some links are manually configured (by the **channel-group** command) and others are dynamically learned in the same channel-group.

Example To enable global passive mode for LACP channel groups, use the command:

```
awplus(config)# lacp global-passive-mode enable
```

To disable global passive mode for LACP channel groups, use the command:

```
awplus(config)# no lacp global-passive-mode enable
```

Related commands show etherchannel

show etherchannel detail

lacp port-priority

Overview Use this command to set the priority of a device port. Ports are selected for aggregation based on their priority, with the higher priority (numerically lower) ports selected first.

Use the **no** variant of this command to reset the priority of port to the default.

Syntax

```
lacp port-priority <1-65535>
no lacp port-priority
```

Parameter	Description
<1-65535>	Specify the LACP port priority.

Default The default is 32768.

Mode Interface Configuration

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lacp port-priority 34
```

lacp system-priority

Overview Use this command to set the system priority of a local system. This is used in determining the system responsible for resolving conflicts in the choice of aggregation groups.

Use the **no** variant of this command to reset the system priority of the local system to the default.

Syntax

```
lacp system-priority <1-65535>
no lacp system-priority
```

Parameter	Description
<1-65535>	LACP system priority. Lower numerical values have higher priorities.

Default The default is 32768.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# lacp system-priority 6700
```

lacp timeout

Overview Use this command to set the short or long timeout on a port. Ports will time out of the aggregation if three consecutive updates are lost.

Syntax

```
lacp timeout {short|long}
```

Parameter	Description
`timeout`	Number of seconds before invalidating a received LACP data unit (DU).
`short`	LACP short timeout. The **short** timeout value is **1** second.
`long`	LACP long timeout. The **long** timeout value is **30** seconds.

Default The default is **long** timeout (30 seconds).

Mode Interface Configuration

Usage notes This command enables the device to indicate the rate at which it expects to receive LACPDUs from its neighbor.

If the timeout is set to **long**, then the device expects to receive an update every **30** seconds, and this will time a port out of the aggregation if no updates are seen for 90 seconds (i.e. 3 consecutive updates are lost).

If the timeout is set to **short**, then the device expects to receive an update every second, and this will time a port a port out of the aggregation if no updates are seen for 3 seconds (i.e. 3 consecutive updates are lost).

The device indicates its preference by means of the Timeout field in the Actor section of its LACPDUs. If the Timeout field is set to 1, then the device has set the **short** timeout. If the Timeout field is set to 0, then the device has set the **long** timeout.

Setting the **short** timeout enables the device to be more responsive to communication failure on a link, and does not add too much processing overhead to the device (1 packet per second).

NOTE: *It is not possible to configure the rate that the device sends LACPDUs; the device must send at the rate which the neighbor indicates it expects to receive LACPDUs.*

Examples The following commands set the LACP long timeout period for 30 seconds on port1.0.2.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lacp timeout long
```

The following commands set the LACP short timeout for 1 second on port1.0.2.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lacp timeout short
```

platform load-balancing

Overview This command selects which address fields are used as inputs into the load balancing algorithm for aggregated links. The output from this algorithm is used to select which individual path a given packet will traverse within an aggregated link.

The **no** variant of this command applies its default setting.

Syntax

```
platform load-balancing {src-dst-mac|src-dst-ip}
no platform load-balancing
```

Parameter	Description
`src-dst-mac`	Include the source and destination MAC addresses (Layer 2)
`src-dst-ip`	Include the source and destination IP addresses (Layer 3) and UDP/TCP source and destination ports. If you choose this option, the algorithm will use MAC addresses to calculate load balancing for Layer 2 and non-IP packets.

Default The default is **src-dst-ip**.

Mode Global configuration

Examples To set the load balancing algorithm to include only Layer 2 MAC addresses, use the commands:

```
awplus# configure terminal
awplus(config)# platform load-balancing src-dst-mac
```

To set the load balancing algorithm to include only Layer 3 IP addresses and Layer 4 ports, use the commands:

```
awplus# configure terminal
awplus(config)# platform load-balancing src-dst-ip
```

Related commands show platform

show debugging lacp

Overview Use this command to see what debugging is turned on for LACP management.

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

Syntax
```
show debugging lacp
```

Mode User Exec and Privileged Exec

Example
```
awplus# show debugging lacp
```

Output Figure 19-1: Example output from the **show debugging lacp** command

```
LACP debugging status:
 LACP timer debugging is on
 LACP timer-detail debugging is on
 LACP cli debugging is on
 LACP packet debugging is on
 LACP event debugging is on
 LACP sync debugging is on
```

Related commands debug lacp

show diagnostic channel-group

Overview This command displays dynamic and static channel group interface status information. The output of this command is useful for Allied Telesis authorized service personnel for diagnostic purposes.

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

Syntax
```
show diagnostic channel-group
```

Mode User Exec and Privileged Exec

Example
```
awplus# show diagnostic channel-group
```

Output Figure 19-2: Example output from the **show diagnostic channel-group** command

```
awplus#show diagnostic channel-group

Channel Group Info based on NSM:
Note: Pos - position in hardware table
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503     port1.0.15   5015     No
     sa3        4503     port1.0.18   5018     No
     po1        4601     port1.0.7    5007     No
     po1        4601     port1.0.8    5008     No
     po1        4601     port1.0.9    5009     No


Channel Group Info based on HSL:
Note: Pos - position in hardware table
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503                           N/a
     po1        4601                           N/a


Channel Group Info based on IPIFWD:
Note: Pos - position in hardware table
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503                           N/a
     po1        4601                           N/a
```

```
Channel Group Info based on HW:
Note: Pos - position in hardware table
      Only entries from first device are displayed.
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503                           N/a
     po1        4601                           N/a


No error found
```

Related commands show tech-support

show etherchannel

Overview Use this command to display information about an LACP channel specified by the channel group number.

The command output also shows the thrash limiting status. If thrash limiting is detected and the **action** parameter of the thrash-limiting command is set to **vlan-disable**, the output will also show the VLANs on which thrashing is detected.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show etherchannel [<1-248>]
```

Parameter	Description
<1-248>	Channel-group number.

Mode User Exec and Privileged Exec

Example

```
awplus# show etherchannel
```

Output Figure 19-3: Example output from **show etherchannel**

```
awplus#show etherchannel
LAG Maximum        : 128
LAG Static  Count  : 0
LAG Dynamic Count  : 1
LAG Total   Count  : 1
Lacp Aggregator: po1
Member:
 port1.0.1
port1.0.2
```

Example

```
awplus# show etherchannel 1
```

Output Figure 19-4: Example output from **show etherchannel** for a particular channel

```
awplus#show etherchannel 1
Aggregator po1 (4601)
 Mac address: 00:00:00:00:00:00
 Admin Key: 0001 - Oper Key 0000
 Receive link count: 0 - Transmit link count: 0
 Individual: 0 - Ready: 0
 Partner LAG: 0x0000,00-00-00-00-00-00
  Link: port1.0.1 (5001) disabled
  Link: port1.0.2 (5002) disabled
```

show etherchannel detail

Overview Use this command to display detailed information about all LACP channels.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show etherchannel detail
```

Mode User Exec and Privileged Exec

Example

```
awplus# show etherchannel detail
```

Output Example output from **show etherchannel detail**

```
awplus#show etherchannel detail
Aggregator po1 (IfIndex: 4601)
 Mac address: 00:00:cd:37:05:17
 Admin Key: 0001 - Oper Key 0001
 Receive link count: 2 - Transmit link count: 2
 Individual: 0 - Ready: 1
 Partner LAG: 0x8000,00-00-cd-37-02-9a,0x0001
  Link: port1.0.1 (IfIndex: 8002) synchronized
  Link: port1.0.2 (IfIndex: 20002) synchronized
Aggregator po2 (IfIndex: 4602)
 Mac address: 00:00:cd:37:05:17
 Admin Key: 0002 - Oper Key 0002
 Receive link count: 2 - Transmit link count: 2
 Individual: 0 - Ready: 1
 Partner LAG: 0x8000,ec-cd-6d-aa-c8-56,0x0002
  Link: port1.0.3 (IfIndex: 8001) synchronized
  Link: port1.0.4 (IfIndex: 20001) synchronized
```

show etherchannel summary

Overview Use this command to display a summary of all LACP channels.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show etherchannel summary
```

Mode User Exec and Privileged Exec

Example

```
awplus# show etherchannel summary
```

Output Example output from **show etherchannel summary**

```
awplus#show etherchannel summary
Aggregator po10 (IfIndex: 4610)
 Admin Key: 0010 - Oper Key 0010
  Link: port1.0.1 (IfIndex: 7007) synchronized
  Link: port1.0.2 (IfIndex: 8007) synchronized
  Link: port1.0.3 (IfIndex: 11007) synchronized
```

show lacp sys-id

Overview Use this command to display the LACP system ID and priority.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show lacp sys-id
```

Mode User Exec and Privileged Exec

Example

```
awplus# show lacp sys-id
```

Output Example output from **show lacp sys-id**

```
System Priority: 0x8000 (32768)
MAC Address: 0200.0034.5684
```

show lacp-counter

Overview Use this command to display the packet traffic on all ports of all present LACP aggregators, or a given LACP aggregator.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show lacp-counter [<1-248>]
```

Parameter	Description
<1-248>	Channel-group number.

Mode User Exec and Privileged Exec

Example

```
awplus# show lacp-counter 2
```

Output Example output from **show lacp-counter**

```
% Traffic statistics
Port           LACPDUs          Marker          Pckt err
            Sent     Recv     Sent     Recv     Sent     Recv
% Aggregator po2 (IfIndex: 4604)
port1.0.2   0        0        0        0        0        0
```

show port etherchannel

Overview Use this command to show LACP details of the device port specified.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show port etherchannel <port>
```

Parameter	Description
<port>	Name of the device port to display LACP information about.

Mode User Exec and Privileged Exec

Example

```
awplus# show port etherchannel port1.0.2
```

Output Example output from **show port etherchannel**

```
awplus#show port etherchannel port1.0.2
LACP link info: port1.0.2 - 7007
Link: port1.0.2 (IfIndex: 7007)
Aggregator: po10 (IfIndex: 4610)
Receive machine state: Current
Periodic Transmission machine state: Slow periodic
Mux machine state: Collecting/Distributing
Actor Information:                      Partner Information:
 Selected ................. Selected     Partner Sys Priority ....... 0x8000
 Physical Admin Key ..... 2             Partner System .. ec-cd-6d-d1-64-d0
 Port Key ..... 10                      Port Key ..... 10
 Port Priority ..... 32768              Port Priority ..... 32768
 Port Number ..... 7007                 Port Number ..... 5001
 Mode ..... Active                      Mode ..... Active
 Timeout ..... Long                     Timeout ..... Long
 Individual ..... Yes                   Individual ..... Yes
 Synchronised ..... Yes                 Synchronised ..... Yes
 Collecting ..... Yes                   Collecting ..... Yes
 Distributing ..... Yes                 Distributing ..... Yes
 Defaulted ..... No                     Defaulted ..... No
 Expired ..... No                       Expired ..... No
```

show static-channel-group

Overview Use this command to display all configured static channel groups and their corresponding member ports. Note that a static channel group is the same as a static aggregator.

The command output also shows the thrash limiting status. If thrash limiting is detected and the **action** parameter of the thrash-limiting command is set to **vlan-disable**, the output will also show the VLANs on which thrashing is detected.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax
```
show static-channel-group
```

Mode User Exec and Privileged Exec

Example
```
awplus# show static-channel-group
```

Output Example output from **show static-channel-group**

```
% LAG Maximum        : 128
% LAG Static  Count  : 2
% LAG Dynamic Count  : 0
% LAG Total   Count  : 2
% Static Aggregator: sa2
% Member:
   port1.0.1
port1.0.2
% Static Aggregator: sa3
% Member:
   port1.0.3
port1.0.4
```

Related commands static-channel-group

static-channel-group

Overview Use this command to create a static channel group, or to add a port to an existing static channel group. Static channel groups are also known as static aggregators.

You can create up to 128 channel groups, in any combination of static and dynamic (LACP) groups. This means you can create up to 128 static channel groups, if you have no dynamic channel groups.

Use the **no** variant of this command to remove the device port from the static channel group.

Syntax

```
static-channel-group <static-channel-group-number>
no static-channel-group
```

Parameter	Description
<static-channel-group-number>	<1-248> Static channel group number. You can create up to 128 static channel groups, numbered in the range 1-248.

Mode Interface Configuration

Usage notes This command adds the device port to the static channel group with the specified channel group number. If the channel group does not exist, it is created, and the port is added to it. The **no** prefix detaches the port from the static channel group. If the port is the last member to be removed, the static channel group is deleted.

All the ports in a channel group must have the same VLAN configuration: they must belong to the same VLANs and have the same tagging status, and can only be operated on as a group.

Once the static channel group has been created, it is treated as a device port. You can specify it in other commands by using **sa** followed by the channel-group number. For example, use the command **show interface sa2** to show details about channel group 2's interface:

Examples To define static channel group 2 on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# static-channel-group 2
```

To reference static channel group 2 as an interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface sa2
awplus(config-if)#
```

Related commands show static-channel-group

Command changes Version 5.4.9-0.1: Ability added to create up to 128 groups as any combination of static and dynamic channel groups. Also, numbering changed to 1-248.

undebug lacp

Overview This command applies the functionality of the no debug lacp command.

20 Power over Ethernet Commands

Introduction

Overview

This chapter contains an alphabetical list of commands used to configure Power over Ethernet (PoE). Each command contains a functional description and shows examples of configuration and output screens for show commands. These commands are only supported on PoE capable ports. An error message will display on the console if you enter a PoE command on a port that does not support PoE. The following documents offer further information for configuring PoE on AlliedWare Plus switches.

- the PoE Feature Overview and Configuration_Guide.
- the Support for Allied Telesis Enterprise_MIBs_in AlliedWare Plus, for information about which PoE MIB objects are supported.
- the SNMP Feature Overview and Configuration_Guide, for information about SNMP traps.

Power over Ethernet (PoE) is a technology allowing devices such as security cameras to receive power over LAN cabling.

The Powered Device (PD) referred to throughout this chapter is a PoE or PoE+ powered device, such as an IP phone or a Wireless Access Point (WAP).

AT-IE300-12GP switches support high-power PoE and offer up to 60W of POE on ports 1.0.9, 1.0.10, 1.0.11 and 1.0.12.

Command List

- "clear power-inline counters interface" on page 787
- "debug power-inline" on page 788
- "power-inline allow-legacy" on page 790
- "power-inline description" on page 791
- "power-inline enable" on page 792
- "power-inline hanp" on page 793
- "power-inline max" on page 794

- "power-inline priority" on page 796
- "power-inline usage-threshold" on page 798
- "power-inline wattage max" on page 799
- "service power-inline" on page 800
- "show debugging power-inline" on page 801
- "show power-inline" on page 802
- "show power-inline counters" on page 806
- "show power-inline interface" on page 808
- "show power-inline interface detail" on page 811

clear power-inline counters interface

Overview This command will clear the counters from a specified port, a range of ports, or all ports on the switch. If no ports are entered then PoE counters for all ports are cleared. It will also clear all Power over Ethernet (PoE) counters supported by the Power Ethernet MIB (RFC 3621).

Syntax

```
clear power-inline counters interface [<port-list>]
```

Parameter	Description
<port-list>	Selects the port or ports whose counters are to be cleared.

Mode Privileged Exec

Usage notes The PoE counters are displayed with the show power-inline counters command.

Examples To clear the PoE counters for port1.0.5 only, use the following command:

```
awplus# clear power-inline counters interface port1.0.5
```

To clear the PoE counters for port1.0.5 through port1.0.8, use the following command:

```
awplus# clear power-inline counters interface
port1.0.5-port1.0.8
```

To clear the PoE counters for all ports, use the following command:

```
awplus# clear power-inline counters interface
```

Related commands show power-inline counters

Command changes Version 5.4.8-0.2: added to x550 series products

debug power-inline

Overview This command enables debugging display for messages that are specific to Power over Ethernet (PoE).

Use the **no** variant of this command to disable the specified PoE debugging messages.

Syntax

```
debug power-inline [all|event|info|power]
no debug power-inline [all|event|info|power]
```

Parameter	Description
`all`	Displays all (`event`, `info`, `nsm`, `power`) debug messages.
`event`	Displays event debug information, showing any error conditions that may occur during PoE operation.
`info`	Displays informational level debug information, showing high-level essential debugging, such as information about message types.
`power`	Displays power management debug information.

Default No debug messages are enabled by default.

Mode Privileged Exec

Usage notes Use the terminal monitor command to display PoE debug messages on the console.

Use the show debugging power-inline command to show the PoE debug configuration.

Examples To enable PoE debugging and start the display of PoE event and info debug messages on the console, use the following commands:

```
awplus# terminal monitor
awplus# debug power-inline event info
```

To enable PoE debugging and start the display of all PoE debugging messages on the console, use the following commands:

```
awplus# terminal monitor
awplus# debug power-inline all
```

To stop the display of PoE info debug messages on the console, use the following command:

```
awplus# no debug power-inline info
```

To disable all PoE debugging and stop the display of any PoE debugging messages on the console, use the following command:

```
awplus# no debug power-inline all
```

Related commands

show debugging power-inline

terminal monitor

Command changes

Version 5.4.8-0.2: added to x550 series products

power-inline allow-legacy

Overview This command enables detection of pre-IEEE 802.3af Power Ethernet standard legacy Powered Devices (PDs).

The **no** variant of this command disables detection of pre-IEEE 802.3af Power Ethernet standard legacy Powered Devices (PDs).

Syntax

```
power-inline allow-legacy
no power-inline allow-legacy
```

Default Detection of legacy PDs is disabled on all ports

Mode Global Configuration

Examples To enable detection of legacy PDs, use the following commands:

```
awplus# configure terminal
awplus(config)# power-inline allow-legacy
```

To disable detection of legacy PDs, use the following commands:

```
awplus# configure terminal
awplus(config)# no power-inline allow-legacy
```

Validation Commands show power-inline

show running-config power-inline

Command changes Version 5.4.8-0.2: added to x550 series products

Version 5.4.9-0.1: default changed to “disabled”

power-inline description

Overview This command adds a description for a Powered Device (PD) connected to a PoE port.

The **no** variant of this command clears a previously entered description for a connected PD, resetting the PD description to the default (null).

Syntax

```
power-inline description <pd-description>
no power-inline description
```

Parameter	Description
<pd-description>	Description of the PD connected to the PoE capable port (with a maximum 256 character string limit per PD description).

Default No description for a connected PD is set by default.

Mode Interface Configuration

Usage notes Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding interface (to configure) command. If you specify a range or list of ports they must all be PoE capable ports.

Examples To add the description "Desk Phone" for a connected PD on port1.0.5, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# power-inline description Desk Phone
```

To clear the description for the connected PD on port1.0.5, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# no power-inline description
```

Related commands show power-inline interface

show running-config *<power-inline>*

Command changes Version 5.4.8-0.2: added to x550 series products

power-inline enable

Overview This command enables Power over Ethernet (PoE) to detect a connected Powered Device (PD) and supply power.

The **no** variant of this command disables PoE functionality on the selected PoE port(s). No power is supplied to a connected PD after PoE is disabled on the selected PoE port(s).

Ports still provide Ethernet connectivity after PoE is disabled.

Syntax
```
power-inline enable
no power-inline enable
```

Default PoE is enabled by default on all ports

Mode Interface Configuration for one or more PoE switchports.

Usage notes No PoE log messages are generated for ports on which PoE is disabled.

Examples To disable PoE on port1.0.5 to port1.0.8, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5-port1.0.8
awplus(config-if)# no power-inline enable
```

To enable PoE on port1.0.5 to port1.0.8, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5-port1.0.8
awplus(config-if)# power-inline enable
```

Related commands

show power-inline

show power-inline interface

show power-inline interface detail

show running-config power-inline

Command changes Version 5.4.8-0.2: added to x550 series products

power-inline hanp

Overview Use this command to enable High Availability Network Power (HANP), also known as Continuous PoE. Continuous PoE enables the switches to perform actions such as software upgrades without forcing the Powered Devices to power cycle. This means, for example, if you are rebooting a switch connected to a PD such as a camera, Continuous PoE allows the camera to buffer while the switch is rebooted. You can configure it on a global or per port level. Enabling it globally enables it on all PoE ports.

Use the **no** variant of this command to disable Continuous PoE globally or on the specified ports.

Syntax

```
power-inline hanp
no power-inline hanp
```

Default Continuous PoE is disabled globally by default. If you enable it globally, that enables it on all ports.

Mode User Exec/Privileged Exec or Interface Configuration for a PoE port

Example To enable Continuous PoE on all ports, use the commands:

```
awplus# configure terminal
awplus(config)# power-inline hanp
```

To enable Continuous PoE on all ports except port 1.0.5, use the commands:

```
awplus# configure terminal
awplus(config)# power-inline hanp
awplus(config)# interface port1.0.5
awplus(config-if)# no power-inline hanp
```

Related commands

show power-inline

show power-inline interface

show power-inline interface detail

Command changes

Version 5.4.6-2.1: command added

Version 5.4.7-0.1: added to x930 series products

Version 5.4.8-0.2: added to x550 series products

Version 5.4.8-2.1: added to x220 series products

power-inline max

Overview This command sets the maximum power allocated to a Power over an Ethernet (PoE and PoE+) port. The amount of power actually supplied to the port depends on the power requirements of the connected PD. It is also a function of the total PoE power loading on the switch and the PoE priority set for the port by the power-inline priority command. However this command (power-inline max) does apply a maximum value to the power that the port is able to supply.

This switch allocates power dynamically, so you do not need to use this command to set it statically. If you do use this command, the values specified in this command will override the dynamic allocation and will control the power output for each port.

Note that the value set by this command will be the figure the switch will use when apportioning the power budget for its ports. For example, if 15.4 W is assigned to a port whose PD only consumes 5 W, the switch will reserve the full 15.4 W for this port when determining its total power PoE power requirement.

The **no** variant of this command sets the maximum power supplied to a PoE port to the default, which is set to the maximum power limit for the class of the connected Powered Device (PD).

Syntax

```
power-inline max <4000-30000>
no power-inline max
```

Parameter	Description
<4000-30000>	The maximum power supplied to a PoE port in milliwatts (mW).

Default By default, the switch dynamically determines the power used by the PD connected to the port.

Mode Interface Configuration for one or more ports. If you specify a range or list of ports, they must all be PoE capable ports.

Usage notes If you select a range of PoE ports in Interface Configuration mode before issuing this command, then each port in the range selected will have the same maximum power value configured.

If a PoE port attempts to draw more than the maximum power, this is logged and all power is removed.

Note that the value entered is rounded up to the next value supported by the hardware. The actual value used is displayed after you enter the command, such as in the following sample console output:

```
awplus#configure terminal

awplus(config)#interface port1.0.5

awplus(config-if)#power-line max 5300

% The maximum power has been rounded to 5450mW in hardware.
```

See the LLDP Feature Overview and Configuration Guide for information about power monitoring at the PD.

Note the difference in power supplied from the PSE to the power available at the PD due to line loss.

See the PoE Feature Overview and Configuration Guide for further information about the difference between the power supplied from the PSE and the power available at the PD.

Examples To set the maximum power supplied to ports in the range port1.0.1 to port1.0.4 to 6450mW per port, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# power-inline max 6450
```

To clear the user-configured maximum power supplied to port1.0.1, and revert to using the default maximum power, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no power-inline max
```

Related commands show power-inline interface

show running-config power-inline

Command changes Version 5.4.8-0.2: added to x550 series products

power-inline priority

Overview This command sets the Power over Ethernet (PoE) priority level of a PoE port to one of three available priority levels:

- low
- high
- critical

The **no** variant of this command restores the PoE port priority to the default (low).

Syntax

```
power-inline priority {low|high|critical}
no power-inline priority
```

Parameter	Description
`low`	The lowest priority for a PoE enabled port (default). PoE ports set to **low** only receive power if all the PoE ports assigned to the other two levels are already receiving power.
`high`	The second highest priority for a PoE enabled port. PoE ports set to **high** receive power only if all the ports set to **critical** are already receiving power.
`critical`	The highest priority for a PoE enabled port. PoE ports set to **critical** are guaranteed power before any ports assigned to the other two priority levels. Ports assigned to the other priority levels receive power only if all critical ports are receiving power.

Default The default priority is **low** for all PoE ports

Mode Interface Configuration

Usage notes Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding interface (to configure) command. If you specify a range or list of ports they must all be PoE capable ports.

PoE ports with higher priorities are given power before PoE ports with lower priorities. If the priorities for two PoE ports are the same then the lower numbered PoE port is given power before the higher numbered PoE port.

See the PoE Feature Overview and Configuration Guide for further information about PoE priority.

Examples To set the priority level to high on port1.0.5 to port1.0.8, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5-port1.0.8
awplus(config-if)# power-inline priority high
```

To reset the priority level to the default of low, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5-port1.0.8
awplus(config-if)# no power-inline priority
```

Related commands

power-inline usage-threshold

show power-inline

show power-inline interface

show running-config power-inline

Command changes

Version 5.4.8-0.2: added to x550 series products

power-inline usage-threshold

Overview This command sets the level at which the switch will issue a message that the power supplied to all Powered Devices (PDs) has reached a critical level of the nominal power rating for the switch. The level is set as a percentage of total available power.

The **no** variant of this command resets the notification usage-threshold to the default (80% of the nominal power rating).

Syntax

```
power-inline usage-threshold <1-99>
no power-inline usage-threshold
```

Parameter	Description
<1-99>	The usage-threshold percentage configured with this command.

Default The default power usage threshold is 80% of the nominal power rating

Mode Global Configuration

Usage notes Use the snmp-server enable trap command to configure SNMP notification. An SNMP notification is sent when the usage-threshold, as configured in the example, is exceeded.

Examples To generate SNMP notifications when power supplied exceeds 70% of the nominal power rating, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap power-inline
awplus(config)# power-inline usage-threshold 70
```

To reset the notification threshold to the default (80% of the nominal power rating), use the following commands:

```
awplus# configure terminal
awplus(config)# no power-inline usage-threshold
```

Related commands snmp-server enable trap

show power-inline interface

show running-config power-inline

Command changes Version 5.4.8-0.2: added to x550 series products

power-inline wattage max

Overview Use this command to specify the maximum system-wide power to be delivered by the switch. This is useful if the switch is powered by a system that cannot deliver the default wattage.

Use the **no** variant of this command to return the maximum power to the default value.

Syntax

```
power-inline wattage max <watts>
no power inline wattage
```

Parameter	Description
`max <watts>`	The maximum number of watts to be distributed by the device, from 1 to 240. Note that you cannot set the wattage to be higher than the switch's system limit of 240W, which is the default value.

Default The switch's system limit, which is 240 watts

Mode Global Configuration

Example To set the switch's maximum wattage to 90W, use the commands:

```
awplus# configure terminal
awplus(config)# power inline wattage max 90
```

Related commands show power-inline

Command changes Version 5.4.6-1.1: command added

service power-inline

Overview This command enables Power over Ethernet (PoE) globally on the switch, for all PoE ports.

Syntax

```
service power-inline
no service power-inline
```

Default PoE functionality is enabled by default

Mode Global Configuration

Examples To disable PoE, use the following commands:

```
awplus# configure terminal
awplus(config)# no service power-inline
```

To re-enable PoE, if PoE has been disabled, use the following commands:

```
awplus# configure terminal
awplus(config)# service power-inline
```

Related commands show power-inline

show running-config power-inline

Command changes Version 5.4.8-0.2: added to x550 series products

show debugging power-inline

Overview This command displays Power over Ethernet (PoE) debug settings.

Syntax

```
show debugging power-inline
```

Mode User Exec and Privileged Exec

Example To display PoE debug settings, use the following command:

```
awplus# show debugging power-inline
```

Output Figure 20-1: Example output from the **show debugging power-inline** command

```
awplus#show debugging power-inline
PoE Debugging status:
PoE Informational debugging is disabled
PoE Event debugging is disabled
PoE Power Management debugging is disabled

PoE NSM debugging is enabled
```

Related commands debug power-inline

terminal monitor

Command changes Version 5.4.8-0.2: added to x550 series products

show power-inline

Overview This command displays the Power over Ethernet (PoE) status for all ports.

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

Syntax
```
show power-inline
```

Mode User Exec and Privileged Exec

Example To display the PoE status for all ports, use the following command:

```
awplus# show power-inline
```

Output Figure 20-2: Example output from **show power-inline**

```
awplus#show power-inline
PoE Status:

 Nominal Power: 240W
 Power Allocated: 15W
 Power Requested: 15W
 Actual Power Consumption: 2W
 Operational Status: On
 Power Usage Threshold: 80% (192W)
 Detection of legacy devices is disabled
 Power Source: AC
 High Availability Network Power: Disabled
 Thermal State: Operational
 Power management mode: Dynamic

PoE Interface:
Interface   Admin    Pri  Oper     Power Device          Class Max
                                    (mW)                      (mW)
port1.0.5   Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.6   Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.7   Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.8   Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.9   Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.10  Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.11  Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.12  Enabled  Low  Powered   1800 n/a                 0 15400 [C]
port1.0.13  Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.14  Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.15  Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.16  Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.17  Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.18  Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.19  Enabled  Low  Off         0 n/a               n/a   n/a
port1.0.20  Enabled  Low  Off         0 n/a               n/a   n/a
```

Table 1: Parameters in the **show power-inline** command output

Parameter	Description
Nominal Power	The nominal power available on the switch in watts (W).
Power Allocated	The current power allocated in watts (W) that is available to be drawn by any connected Powered Devices (PDs). This is updated every 5 seconds.
Actual Power Consumption	The current power consumption in watts (W) drawn by all connected Powered Devices (PDs). This is updated every 5 seconds.
Operational Status	The operational status of the PSU hardware when this command was issued: • **On** if the PSU is installed and switched on. • **Off** when the PSU is switched off (an RPS may be connected to the switch to power PoE instead of the PSU). • **Fault** when there is an issue with the PSU hardware.
Power Usage Threshold (%)	The configured SNMP trap / log threshold, as configured from a power-inline usage-threshold command.
Power management mode: Dynamic	Indicates that PoE power is allocated dynamically, based on the current usage of each PD attached to the switch's ports. When you connect a new PD to the switch, the switch determines whether it can power that device by measuring the power the existing PDs are currently using. If there is sufficient power available, the switch will allocate it to the new device.
High Availability Network Power	Whether High Availability Network Power is enabled or disabled globally. HANP is also known as Continuous PoE. Continuous PoE enables the switch to perform actions such as software upgrades without forcing the Powered Devices to power cycle. This allows, for example, IP cameras to buffer data instead of losing it.
Thermal State	Whether the switch has exceeded its safe operational temperature and removed power from some or all ports to limit over-heating: • **Operational** means that the switch has not removed power from any ports. • **Non-Critical Ports Denied** means that the switch has stopped supplying power to all ports except those with a priority setting of Critical. • **All Ports Denied** means that the switch has stopped supplying power to all ports. If the switch has stopped supplying power to any ports, it will start supplying power again automatically when the temperature returns to a safe level.

Table 1: Parameters in the **show power-inline** command output (cont.)

Parameter	Description
Interface	The PoE port(s) in the format portx.y.z, where x is the device number, y is the module number within the device, and z is the PoE port number within the module.
Admin	The administrative state of PoE on a PoE port, either **Enabled** or **Disabled**.
Pri	The current PoE priorities for PoE ports, as configured using the power-inline priority command: • **Low** is the lowest priority (this is the default). • **High** is the second highest priority. • **Crit** (critical) is the highest priority. If the switch cannot supply all ports, it will supply critical ports, then high-priority ports, then low-priority ports.
Oper	The current PoE port state when this command was issued: • **Powered** displays if there is a PD connected and power is being supplied. • **Denied** displays if supplying power would make the switch go over the power budget. It also displays if the switch is overheating and therefore has stopped supplying power to the port. • **Off** displays if the port is not supplying power but has not been denied power by the switch. This is the default state for ports that are not connected to a PD. • **Disabled** displays if the PoE port is administratively disabled. • **Syncing** displays if PoE is still initializing the port when you issue the command. • **Fault** displays if there is a problem with PoE on the port. • **Unknown** displays if PoE cannot determine the state of the port.
Power	The power consumption in milliwatts (mW) for the PoE port when this command was entered.
Device	The description of the connected PD device if a description has been added with the power-inline description command. No description is shown for PDs not configured with the power-inline description command.
Class	The class of the connected PD, if power is being supplied to the PD.

Table 1: Parameters in the **show power-inline** command output (cont.)

Parameter	Description
Max (mW)	The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port: • **[U]** if the power limit for a port was user configured (with the power-inline max command). • **[L]** if the power limit for a port was supplied by LLDP. • **[C]** if the power limit for a port was supplied by the PD class.
HANP	Whether High Availability Network Power is enabled (on) or not (off) on the port. HANP is also known as Continuous PoE. Continuous PoE enables the switch to perform actions such as software upgrades without forcing the Powered Devices to power cycle. This allows, for example, IP cameras to buffer data instead of losing it. This column only displays if Continuous PoE has been enabled globally on the switch.

Related commands

show power-inline counters

show power-inline interface

Command changes

Version 5.4.8-0.2: added to x550 series products

show power-inline counters

Overview This command displays Power over Ethernet (PoE) event counters for ports on the Power Sourcing Equipment (PSE). The PoE event counters displayed can also be accessed by objects in the PoE MIB (RFC 3621). See the MIB Objects Feature Overview and Configuration Guide for information about which PoE MIB objects are supported.

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

Syntax

```
show power-inline counters [<port-list>]
```

Parameter	Description
<port-list>	Enter the PoE port(s) to display PoE event counters for them.

Mode User Exec and Privileged Exec

Examples To display all PoE event counters for all PoE ports, use the command:

```
awplus# show power-inline counters
```

To display the PoE event counters for port1.0.5, use the command:

```
awplus# show power-inline counters port1.0.5
```

Output Figure 20-3: Example output from the **show power-inline counters** command

```
awplus#show power-inline counters
PoE Counters:
Interface   MPSAbsent Overload Short Invalid Denied
port1.0.1   0         0        0     0       0
port1.0.2   0         0        0     0       0
port1.0.3   0         0        0     0       0
port1.0.4   0         0        0     0       0
port1.0.5   0         0        0     0       0
...
```

Table 2: Parameters in the **show power-inline counters** command output

Parameter	Description
`Interface`	The PoE port(s) in the format portx.y.z, where x is the device number, y is the module number within the device, and z is the PoE port number within the module.
`MPSAbsent`	The number of instances when the PoE MPS (Maintain Power Signature) signal has been lost. The PoE MPS signal is lost when a PD is disconnected from the PSE. Also increments `pethPsePortMPSAbsentCounter` in the PoE MIB.

Table 2: Parameters in the **show power-inline counters** command output

Parameter	Description
`Overload`	The number of instances when a PD exceeds its configured power limit (as configured by the power-inline max command). Also increments `pethPsePortOverLoadCounter` in the PoE MIB.
`Short`	The number of short circuits that have happened with a PD. Also increments `pethPsePortShortCounter` in the PoE MIB.
`Invalid`	The number of times a PD with an Invalid Signature (where the PD has an open or short circuit, or is a legacy PD) is detected. Also increments `pethPseInvalidSignatureCounter` in the PoE MIB.
`Denied`	The number of times a PD has been refused power due to power budget limitations for the PSE. Also increments `pethPsePortPowerDeniedCounter` in the PoE MIB.

Related commands

clear power-inline counters interface

show power-inline

show power-inline interface

Command changes

Version 5.4.8-0.2: added to x550 series products

show power-inline interface

Overview This command displays a summary of Power over Ethernet (PoE) information for specified ports. If no ports are specified then PoE information is displayed for all ports.

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

Syntax

```
show power-inline interface [<port-list>]
```

Parameter	Description
<port-list>	Enter the PoE port(s) to display PoE specific information in the show output.

Mode User Exec and Privileged Exec

Example To display the PoE port-specific information for all PoE ports on the switch, use the following command:

```
awplus# show power-inline interface
```

To display the PoE port specific information for port1.0.5 to port1.0.7, use the following command:

```
awplus# show power-inline interface port1.0.5-port1.0.7
```

Output Figure 20-4: Example output from **show power-inline interface**

```
awplus#show power-inline interface
Interface   Admin    Pri  Oper     Power Device          Class Max
                                    (mW)                      (mW)
port1.0.5   Enabled  Low  Off          0 n/a               n/a   n/a
port1.0.6   Enabled  Low  Off          0 n/a               n/a   n/a
port1.0.7   Enabled  Low  Off          0 n/a               n/a   n/a
port1.0.8   Enabled  Low  Off          0 n/a               n/a   n/a
port1.0.9   Enabled  Low  Off          0 n/a               n/a   n/a
port1.0.10  Enabled  Low  Off          0 n/a               n/a   n/a
port1.0.11  Enabled  Low  Off          0 n/a               n/a   n/a
port1.0.12  Enabled  Low  Powered   1800 n/a                 0 15400 [C]
port1.0.13  Enabled  Low  Off          0 n/a               n/a   n/a
```

Table 3: Parameters in **show power-inline interface** output

Parameter	Description
`Interface`	The PoE port(s) in the format port1.0.z, where z is the port number. After the port number, "/D" indicates the data pair and "/S" indicates the spare pair (for ports that support high-power PoE).
`Admin`	The administrative state of PoE on a PoE port, either **Enabled** or **Disabled**.
`Pri`	The current PoE priorities for PoE ports on the PSE, as configured from a power-inline priority command: • **Low** displays when the `low` parameter is issued. The lowest priority for a PoE enabled port (default). • **High** displays when the `high` parameter is issued. The second highest priority for a PoE enabled port. • **Crit** displays when the `critical` parameter is issued. The highest priority for a PoE enabled port.
`Oper`	The current PoE port state when this command was issued: • **Powered** displays if there is a PD connected and power is being supplied. • **Denied** displays if supplying power would make the switch go over the power budget. It also displays if the switch is overheating and therefore has stopped supplying power to the port. • **Off** displays if the port is not supplying power but has not been denied power by the switch. This is the default state for ports that are not connected to a PD. • **Disabled** displays if the PoE port is administratively disabled. • **Syncing** displays if PoE is still initializing the port when you issue the command. • **Fault** displays if there is a problem with PoE on the port. • **Unknown** displays if PoE cannot determine the state of the port.
`Power`	The power consumption in milliwatts (mW) for the PoE port when this command was entered.
`Device`	The description of the connected PD device if a description has been added with the power-inline description command. No description is shown for PDs not configured with the power-inline description command.
`Class`	The class of the connected PD, if power is being supplied to the PD from the PSE. See the PoE Feature Overview and Configuration Guide for further information about power classes.

Table 3: Parameters in **show power-inline interface** output (cont.)

Parameter	Description
`Max (mW)`	The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following is displayed per PoE port: • **[U]** if the power limit for a port was user configured (with the power-inline max command). • **[L]** if the power limit for a port was supplied by LLDP. • **[C]** if the power limit for a port was supplied by the PD class.
`HANP`	Whether High Availability Network Power is enabled (on) or not (off) on the port. HANP is also known as Continuous PoE. It enables the switch to perform actions such as software upgrades without forcing the Powered Devices to power cycle. This allows, for example, IP cameras to buffer data instead of losing it. This column only displays if Continuous PoE has been enabled globally on the switch.

Related commands

show power-inline

show power-inline interface detail

Command changes

Version 5.4.8-0.2: added to x550 series products

show power-inline interface detail

Overview This command displays detailed information for one or more Power over Ethernet (PoE) ports.

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

Syntax

```
show power-inline interface [<port-list>] detail
```

Parameter	Description
<port-list>	Enter the PoE port(s) to display information about only the specified port or ports.

Mode User Exec and Privileged Exec

Usage notes The power allocated to each port is listed in the **Power allocated** row, and is limited by the maximum power per Powered Device (PD) class, or a user configured power limit.

Examples To display detailed PoE port specific information for the port range port1.0.5 to port1.0.6, use the command:

```
awplus# show power-inline interface port1.0.5-port1.0.6 detail
```

Output Figure 20-5: Example output from **show power-inline interface detail**

```
awplus#show power-inline interface port1.0.5-1.0.6 detail

Interface port1.0.5
  Powered device type: n/a
  PoE admin: on
  Configured Priority: Low
  Actual Priority: Low
  Detection status: Off
  Powered pairs: Data

Interface port1.0.6
  Powered device type: n/a
  PoE admin: on
  Configured Priority: Low
  Actual Priority: Low
  Detection status: Off
  Powered pairs: Data
```

Table 4: Parameters in **show power-inline interface detail** output

Parameter	Description
`Interface`	The PoE port(s) in the format portx.y.z, where x is the device number, y is the module number within the device, and z is the PoE port number within the module.
`Powered device type:`	The name of the PD, if connected and if power is being supplied to the PD from the PSE, configured with the power-inline description command. **n/a** displays if a description has not been configured for the PD.
`PoE admin`	The administrative state of PoE on a PoE capable port, either **Enabled** or **Disabled** as configured from the power-inline enable command or the **no power-inline enable** command respectively.
`Priority`	The PoE priority of a port, which is either **Low,** or **High,** or **Critical**, as configured by the power-inline priority command.
`Detection status:`	The current PSE PoE port state when this command was issued: • **Powered** displays when there is a PD connected and power is being supplied from the PSE. • **Denied** displays when supplying power would make the PSE go over the power budget. • **Disabled** displays when the PoE port is administratively disabled. • **Off** displays when PoE has been disabled for the port. • **Fault** displays when a PSE goes over its power allocation.
`High Availability Network Power:`	Whether HANP is enabled or disabled on the port. HANP is also known as Continuous PoE. It enables the switch to perform actions such as software upgrades without forcing the Powered Devices to power cycle. This allows, for example, IP cameras to buffer data instead of losing it. Note that this information is only displayed if Continuous PoE is enabled globally on the switch.
`Current power consumption:`	The power consumption for the PoE port when this command was entered. Note that the power consumption may have changed since the command was entered and the power is displayed.
`Powered device class:`	The class of the connected PD if connected, and if power is being supplied to the PD from the PSE. See the PoE Feature Overview and Configuration Guide for further information about power classes.
`Power allocated`	The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port: • **[U]** if the power limit for a port was user configured (with the **power-inline max** command). • **[L]** if the power limit for a port was supplied by LLDP. • **[C]** if the power limit for a port was supplied by the PD class.

Table 4: Parameters in **show power-inline interface detail** output (cont.)

Parameter	Description
`Detection of legacy devices is`	The status of legacy PoE detection on the PoE port (enabled or disabled), as configured for the PoE port with the power-inline allow-legacy command. Legacy detection involves measuring for a large capacitance value to confirm the presence of a legacy PD.
`Powered pairs`	The IEEE 802.3af and IEEE 802.3at standards allow for either **data** or **spare** twisted pairs to be used to transfer power to a PD.

Related commands

show power-inline

show power-inline interface

Command changes

Version 5.4.8-0.2: added to x550 series products

21 GVRP Commands

Introduction

Overview

With GVRP enabled the switch can exchange VLAN configuration information with other GVRP enabled switches. VLANs can be dynamically created and managed through trunk ports.

- There is a limit of 400 VLANs supported by the AlliedWare Plus GVRP implementation. VLANs may be numbered 1-4094, but a limit of 400 of these VLANs are supported.
- MSTP is not supported by the AlliedWare Plus GVRP implementation. GVRP and MSTP are mutually exclusive. STP and RSTP are supported by GVRP.

This chapter provides an alphabetical reference for commands used to configure GVRP. For information about GVRP, including configuration, see the GVRP Feature Overview and Configuration Guide.

Command List

- "clear gvrp statistics" on page 815
- "debug gvrp" on page 816
- "gvrp (interface)" on page 818
- "gvrp dynamic-vlan-creation" on page 819
- "gvrp enable (global)" on page 820
- "gvrp registration" on page 821
- "gvrp timer" on page 822
- "show debugging gvrp" on page 824
- "show gvrp configuration" on page 825
- "show gvrp machine" on page 826
- "show gvrp statistics" on page 827
- "show gvrp timer" on page 828

clear gvrp statistics

Overview Use this command to clear the GVRP statistics for all switchports, or for a specific switchport.

Syntax

```
clear gvrp statistics {all|<interface>}
```

Parameter	Description
`all`	Specify all switchports to clear GVRP statistics.
`<interface>`	Specify the switchport to clear GVRP statistics.

Mode Privileged Exec

Usage notes Use this command together with the show gvrp statistics command to troubleshoot GVRP.

Examples To clear all GVRP statistics for all switchport on the switch, enter the command:

```
awplus# clear gvrp statistics all
```

To clear GVRP statistics for switchport interface `port1.0.3`, enter the command:

```
awplus# clear gvrp statistics port1.0.3
```

Related commands show gvrp statistics

debug gvrp

Overview Use this command to debug GVRP packets and commands, sending output to the console.

Use the **no** variant of this command to turn off debugging for GVRP packets and commands.

Syntax

```
debug gvrp {all|cli|event|packet}
no debug gvrp {all|cli|event|packet}
```

Parameter	Description
`all`	Specifies debugging for all levels.
`cli`	Specifies debugging for commands.
event	Specified debugging for events.
`packet`	Specifies debugging for packets.

Mode Privileged Exec and Global Configuration

Examples To enable GVRP on interfaces `port1.0.1-port1.0.2`, enter the commands:

```
awplus# configure terminal
awplus(config)# gvrp enable
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# gvrp
```

To disable GVRP on interfaces `port1.0.1-port1.0.2`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# no gvrp
```

Examples To send debug output to the console for GVRP packets and GVRP commands, and to enable the display of debug output on the console first, enter the commands:

```
awplus# terminal monitor
awplus# configure terminal
awplus(config)# debug gvrp all
```

To send debug output for GVRP packets to the console, enter the commands:

```
awplus# terminal monitor
awplus# configure terminal
awplus(config)# debug gvrp packets
```

To send debug output for GVRP commands to the console, enter the commands:

```
awplus# terminal monitor
awplus# configure terminal
awplus(config)# debug gvrp cli
```

To stop sending debug output for GVRP packets and GVRP commands to the console, and to stop the display of any debug output on the console, enter the commands:

```
awplus# terminal no monitor
awplus# configure terminal
awplus(config)# no debug gvrp all
```

Related commands

show debugging gvrp

terminal monitor

gvrp (interface)

Overview Use this command to enable GVRP for switchport interfaces.

Use the **no** variant of this command to disable GVRP for switchport interfaces.

Syntax

```
gvrp
no gvrp
```

Mode Interface Configuration (for switchport interfaces).

Default Disabled by default.

Usage notes Use this command to enable GVRP on switchport interfaces. Note this command does not enable GVRP for the switch. To enable GVRP on switchports use this command in Interface Configuration mode. You must issue a gvrp enable (global) command before issuing a gvrp (interface) command.

You must enable GVRP on both ends of a link for GVRP to propagate VLANs between links.

NOTE: *MSTP is not supported by the current AlliedWare Plus GVRP implementation. GVRP and MSTP are mutually exclusive. STP and RSTP are supported by GVRP.*

Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. GVRP and private VLAN trunk ports are mutually exclusive.

Examples To enable GVRP on interfaces port1.0.1-port1.0.2, enter the commands:

```
awplus# configure terminal
awplus(config)# gvrp enable
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# gvrp
```

To disable GVRP on interfaces port1.0.1-port1.0.2, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# no gvrp
```

Validation Commands show gvrp configuration

Related commands gvrp dynamic-vlan-creation

gvrp enable (global)

gvrp dynamic-vlan-creation

Overview Use this command to enable dynamic VLAN creation globally for the switch.

Use the **no** variant of this command to disable dynamic VLAN creation globally for the switch.

Syntax

```
gvrp dynamic-vlan-creation
no gvrp dynamic-vlan-creation
```

Mode Global Configuration

Default Disabled by default.

Usage notes You must enable GVRP on both ends of a link for GVRP to propagate VLANs between links.

You must also enable GVRP globally in Global Configuration mode before enabling GVRP on an interface in Interface Configuration mode. Both of these tasks must occur to create VLANs.

NOTE: *There is limit of 400 VLANs supported by the AlliedWare Plus GVRP implementation. VLANs may be numbered 1-4094, but a limit of 400 of these VLANs are supported.*

Examples Enter the following commands for switches with hostnames `switch1` and `switch2` respectively, so `switch1` propagates VLANs to `switch2` and `switch2` propagates VLANs to `switch1`:

Switch1:

```
switch1# configure terminal
switch1(config)# gvrp enable
switch1(config)# gvrp dynamic-vlan-creation
```

Switch2:

```
switch2# configure terminal
switch2(config)# gvrp enable
switch2(config)# gvrp dynamic-vlan-creation
```

To disable GVRP dynamic VLAN creation on the switch, enter the commands:

```
awplus# configure terminal
awplus(config)# no gvrp dynamic-vlan-creation
```

Validation Commands show gvrp configuration

Related commands gvrp enable (global)

gvrp enable (global)

Overview Use this command to enable GVRP globally for the switch.

Use the **no** variant of this command to disable GVRP globally for the switch.

Syntax

```
gvrp enable
no gvrp enable
```

Mode Global Configuration

Default Disabled by default.

Usage notes Use this command to enable GVRP on the switch. Note that this command does not enable GVRP on switchports. To enable GVRP on switchports use the gvrp (interface) command in Interface Configuration mode. You must issue a gvrp enable (global) command before issuing a gvrp (interface) command.

You must enable GVRP on both ends of a link for GVRP to propagate VLANs between links.

NOTE: *MSTP is not supported by the current AlliedWare Plus GVRP implementation. GVRP and MSTP are mutually exclusive. STP and RSTP are supported by GVRP.*

Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. GVRP and private VLAN trunk ports are mutually exclusive.

Examples To enable GVRP for the switch, before enabling GVRP on switchports, enter the commands:

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

To disable GVRP on the switch, which will also disable GVRP enabled on switchports, enter the commands:

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

Validation Commands show gvrp configuration

Related commands gvrp (interface)

gvrp dynamic-vlan-creation

gvrp registration

Overview Use this command to set GVRP registration to normal, fixed, and forbidden registration modes.

Use the **no** variant of this command to disable GVRP registration.

Syntax

```
gvrp registration {normal|fixed|forbidden}
no gvrp registration {normal|fixed|forbidden}
```

Parameter	Description
`normal`	Specify dynamic GVRP registration and deregistration of VLANs.
`fixed`	Specify fixed GVRP registration and deregistration of VLANs.
`forbidden`	Specify no GVRP registration of VLANs. VLANs are deregistered.

Mode Interface Configuration

Default Normal registration is the default.

Usage notes Configuring a trunk port in normal registration mode allows dynamic creation of VLANs. Normal mode is the default mode. Validate using the show gvrp configuration command.

Configuring a trunk port in fixed registration mode allows manual creation of VLANs.

Configuring a trunk port in forbidden registration mode prevents VLAN creation on the port.

Examples To configure GVRP registration to fixed on port1.0.1, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# gvrp registration fixed
```

To disable GVRP registration on interfaces port1.0.1, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no gvrp registration
```

Validation Commands show gvrp configuration

gvrp timer

Overview Use this command to set GVRP timers in Interface Configuration mode for a given interface.

Use the **no** variant of this command to reset the GVRP timers to the defaults specified in the table below.

Syntax

```
gvrp timer {join <timer-value>|leave <timer-value>|leaveall
<timer-value>}
```

```
no gvrp timer {join|leave|leaveall}
```

Parameter	Description
`join`	Specifies the timer for joining the group (default is 20 centiseconds / hundredths of a second, or 200 milliseconds).
`leave`	Specifies the timer for leaving a group (default is 60 centiseconds / hundredths of a second, or 600 milliseconds).
`leaveall`	Specifies the timer for leaving all groups (default is 1000 centiseconds / hundredths of a second, or 10,000 milliseconds).
<timer-value>	<1-65535> The timer value in hundredths of a second (centiseconds).

Mode Interface Configuration

Defaults The default join time value is 20 centiseconds (200 milliseconds), the default leave timer value is 60 centiseconds (600 milliseconds), and the default leaveall timer value is 1000 centiseconds (10,000 milliseconds).

Usage notes When configuring the `leave` timer, set it to more than or equal to three times the `join` timer value. The settings for the `leave` and `join` timers must be the same for all GVRP enabled switches. See also the section "Setting the GVRP Timers" in the GVRP Feature Overview and Configuration Guide.

Use the show gvrp timer command to confirm GVRP timers set with this command.

Examples To set the GVRP join timer to 30 hundredths of a second (300 milliseconds) for interface port1.0.1, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# gvrp timer join 30
```

To set the GVRP leave timer to 90 hundredths of a second (900 milliseconds) for interface port1.0.1, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# gvrp timer leave 90
```

To reset the GVRP join timer to its default of 20 hundredths of a second for interface port1.0.1, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no gvrp timer join
```

Related commands show gvrp timer

show debugging gvrp

Overview Use this command to see what debugging is turned on for GVRP.

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

Syntax

```
show debugging gvrp
```

Mode User Exec and Privileged Exec

Example Enter the following commands to display GVRP debugging output on the console:

```
awplus# configure terminal
awplus(config)# debug gvrp all
awplus(config)# exit
awplus# show debugging gvrp
```

Output See sample output from the **show debugging gvrp** command after entering **debug gvrp all**:

```
GVRP debugging status:
  GVRP Event debugging is on
  GVRP CLI debugging is on
  GVRP Timer debugging is on
  GVRP Packet debugging is on
```

Related commands debug gvrp

show gvrp configuration

Overview Use this command to display GVRP configuration data for a switch.

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

Syntax

```
show gvrp configuration
```

Mode User Exec and Privileged Exec

Example To show GVRP configuration for the switch, enter the command:

```
awplus# show gvrp configuration
```

Output The following is an output of this command displaying the GVRP configuration for a switch:

```
awplus#show gvrp configuration
Global GVRP Configuration:
GVRP Feature: Enabled
Dynamic Vlan Creation: Disabled
Port based GVRP Configuration:
                                          Timers(centiseconds)
Port    GVRP Status Registration  Applicant   Join   Leave LeaveAll
-----------------------------------------------------------------
port1.0.1 Enabled   Normal        Normal      20      60    1000
port1.0.2 Enabled   Normal        Normal      200    600   10000
```

show gvrp machine

Overview Use this command to display the state machine for GVRP.

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

Syntax

```
show gvrp machine
```

Mode User Exec and Privileged Exec

Example To show the GVRP state machine for the switch, enter the command:

```
awplus# show gvrp machine
```

Output See the following output of this command displaying the GVRP state machine.

```
awplus  show gvrp machine
  port = 1.0.1  applicant state = QA   registrar state = INN
  port = 1.0.2  applicant state = QA   registrar state = INN
```

show gvrp statistics

Overview Use this command to display a statistical summary of GVRP information for the switch.

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

Syntax

```
show gvrp statistics [<interface>]
```

Parameter	Description
<interface>	The name of the switchport interface.

Mode User Exec and Privileged Exec

Usage notes Use this command together with the clear gvrp statistics command to troubleshoot GVRP.

Examples To show the GVRP statistics for all switchport interfaces, enter the command:

```
awplus# show gvrp statistics
```

To show the GVRP statistics for switchport interfaces port1.0.1 and port1.0.2, enter the command:

```
awplus# show gvrp statistics port1.0.1-port1.0.2
```

Output The following is an output of this command displaying a statistical summary for port1.0.1-port1.0.2

```
awplus#  show gvrp statistics port1.0.1-port1.0.2
Port     JoinEmpty    JoinIn   LeaveEmpty     LeaveIn     Empty
-----------------------------------------------------------------
1.0.1    RX           0          2          0         0         0
         TX           0          0          0         0         0
1.0.2    RX           0          1          0         0         1
         TX           0          0          0         0         0
```

Related commands clear gvrp statistics

show gvrp timer

Overview Use this command to display data for the GVRP timers set with the gvrp timer command.

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

Syntax

```
show gvrp timer <interface>
```

Parameter	Description
<interface>	The name of the switchport interface.

Mode User Exec and Privileged Exec

Examples To show the GVRP timers for all switchport interfaces, enter the command:

```
awplus# show gvrp timer
```

To show the GVRP timers for switchport interface port1.0.1, enter the command:

```
awplus# show gvrp timer port1.0.1
```

Output The following show output displays data for timers on the switchport interface port1.0.1

```
awplus#  show gvrp timer port1.0.1
Timer           Timer Value (centiseconds)
----------------------------------------
Join                 20
Leave                60
Leave All            1000
```

Related commands gvrp timer

Part 3: Layer 3 Switching

22 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)
- ICMP Router Discovery Advertisements (IRDP)

For more information, see the IP Feature Overview and Configuration Guide.

Command List

- "arp-aging-timeout" on page 832
- "arp-mac-disparity" on page 833
- "arp" on page 836
- "arp log" on page 838
- "arp opportunistic-nd" on page 841
- "arp-reply-bc-dmac" on page 842
- "clear arp-cache" on page 843
- "debug ip packet interface" on page 844
- "debug ip irdp" on page 846
- "ip address (IP Addressing and Protocol)" on page 847
- "ip directed-broadcast" on page 849
- "ip forwarding" on page 851
- "ip forward-protocol udp" on page 852
- "ip gratuitous-arp-link" on page 854
- "ip helper-address" on page 856
- "ip irdp" on page 858
- "ip icmp error-interval" on page 859

- "ip irdp address preference" on page 860
- "ip irdp broadcast" on page 861
- "ip irdp holdtime" on page 862
- "ip irdp lifetime" on page 863
- "ip irdp maxadvertinterval" on page 864
- "ip irdp minadvertinterval" on page 866
- "ip irdp multicast" on page 868
- "ip irdp preference" on page 869
- "ip limited-local-proxy-arp" on page 870
- "ip local-proxy-arp" on page 871
- "ip proxy-arp" on page 872
- "ip redirects" on page 873
- "ip tcp synack-retries" on page 874
- "ip unreachables" on page 875
- "local-proxy-arp" on page 877
- "optimistic-nd" on page 878
- "ping" on page 879
- "router ip irdp" on page 880
- "show arp" on page 881
- "show debugging ip packet" on page 882
- "show ip flooding-nexthops" on page 883
- "show ip forwarding" on page 884
- "show ip interface" on page 885
- "show ip irdp" on page 886
- "show ip irdp interface" on page 887
- "show ip sockets" on page 889
- "show ip traffic" on page 892
- "tcpdump" on page 894
- "traceroute" on page 895
- "undebug ip packet interface" on page 896
- "undebug ip irdp" on page 897

arp-aging-timeout

Overview This command sets a timeout period on dynamic ARP entries associated with a specific interface. If your device stops receiving traffic for the host specified in a dynamic ARP entry, it deletes the ARP entry from the ARP cache after this timeout is reached.

Your device times out dynamic ARP entries to ensure that the cache does not fill with entries for hosts that are no longer active. Static ARP entries are not aged or automatically deleted.

By default the time limit for dynamic ARP entries is 300 seconds on all interfaces.

The **no** variant of this command sets the time limit to the default of 300 seconds.

Syntax

```
arp-aging-timeout <0-432000>
no arp-aging timeout
```

Parameter	Description
<0-432000>	The timeout period in seconds.

Default 300 seconds (5 minutes)

Mode Interface Configuration for VLAN interfaces.

Example To set the ARP entries on interface vlan2 to time out after two minutes, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp-aging-timeout 120
```

Related commands

clear arp-cache

show arp

arp-mac-disparity

Overview Use this command to enable the switch to support services like Microsoft Network Load Balancing (MS-NLB).

Such services use ARP with disparate MAC addresses to ensure that packets destined for a server cluster virtual address are sent to all servers in the cluster. Disparate MAC addresses mean that the MAC address in the "sender hardware address" field of an ARP reply is different to the MAC address in the "Source MAC address" field of the Ethernet header that the ARP packet is encapsulated in.

The **no** variant of this command reverts to the default behavior. See the Default section below for more information.

Syntax

```
arp-mac-disparity {multicast|multicast-igmp|unicast}
no arp-mac-disparity {multicast|multicast-igmp|unicast}
```

Parameter	Description
`multicast`	Enables support of server clusters operating in multicast mode. Packets destined for the server cluster are flooded to all ports in the VLAN.
`multicast-igmp`	Enables support of server clusters operating in multicast/IGMP mode. In multicast/IGMP mode, the MS-NLB server cluster uses IGMP reports to forward server traffic to a limited set of ports.
`unicast`	Enables support of server clusters operating in unicast mode. Packets destined for the server cluster are flooded to all ports in the VLAN.

Default ARP-MAC disparity support is disabled and:

- If the Disparate ARP has a multicast MAC address in the ARP reply, the switch drops the ARP reply and does not learn any associated addresses
- If the Disparate ARP has a unicast MAC address in the ARP reply, the switch learns the address in the ARP reply. The learned ARP entry points to the single port that the ARP reply arrived on. Matching traffic will go out this port.

Mode Interface Configuration for a VLAN interface.

Usage notes

Multicast mode

When you are using **multicast** mode, you can limit the number of ports that packets are flooded to, instead of flooding to all ports in the VLAN. To do this, specify the list of ports when creating the ARP entry.

For example, to flood only port1.0.1 to port1.0.3, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp-mac-disparity multicast
awplus(config-if)# arp 10.10.1.100 010e.11ff.2222
port1.0.1-port1.0.3
```

Multicast IGMP mode

You can enable Multicast-IGMP mode by using the command **arp-mac-disparity multicast-igmp**.

In this mode, the only difference to standard multicast mode is that the reception of IGMP reports now controls the ports to which the L3 switch floods traffic. That is, rather than simply flooding each packet destined for the NLB cluster IP address to all ports on the egress VLAN, those packets are only sent to the switchports in the VLAN that have received IGMP reports for the multicast group corresponding to the NLB cluster MAC address.

Like **arp-mac-disparity multicast**, the command **arp-mac-disparity multicast-igmp** puts the switch into a mode where it will accept Disparate ARP responses. Similarly, upon receiving a Disparate ARP response, an ARP entry is created for the IP/MAC in the content of the ARP packet. The difference with the **arp-mac-disparity multicast-igmp** command is that the egress port is set to the subset of ports in the VLAN that have received IGMP reports for the NLB cluster MAC address.

Note that the ARP entry is updated as ports join/leave the IGMP group. If no ports have received IGMP reports for the NLB cluster MAC address then the ARP entry will have no egress ports and will simply drop packets destined for the NLB cluster IP address.

Again, no FDB entry is created in response to receiving the ARP packet. However, since the NLB server is operating in multicast mode with the IGMP option set and is sending IGMP reports, an FDB entry will already exist for the IGMP group (and, as a result, the NLB cluster MAC address).

When the **arp-mac-disparity multicast-igmp** command is configured on the VLAN, ARP entries appear in the output of the command **show arp** like this:

```
awplus#show arp
IP Address    MAC Address      Interface  Port         Type
10.100.0.56   0100.5e7f.0038   vlan200    igmp-group   dynamic
```

Examples To enable support for MS-NLB in unicast mode on interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp-mac-disparity unicast
```

To disable support for MS-NLB in unicast mode on interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no arp-mac-disparity unicast
```

Related commands

arp

clear arp-cache

show arp

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]
arp <ip-addr> <multicast-mac-address> [<port-list>]
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.
<port-number>	The port number associated with the IP address. Specify this when the IP address is part of a VLAN.
<multicast-mac-address>	The multicast MAC address for which you are adding a static ARP entry, in hexadecimal notation with the format HHHH.HHHH.HHHH.
<port-list>	The list of port numbers associated with the IP address. You can only specify multiple egress ports when the MAC address is a multicast MAC address.
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

Usage notes One use of this command is to limit packet flooding when using services like Microsoft Network Load Balancing (MS-NLB). With such services, packets destined for server cluster virtual address must be sent to all servers in the cluster. The server cluster can operate in multicast mode, in which it uses a multicast MAC address. To support this, this command allows you to create a static ARP entry with a multicast MAC address, and specify which ports the packets will be forwarded out.

Creating a static ARP entry enables the switch to correctly forward server cluster traffic. If you want the switch to also respond to pings from the server cluster, you need to also enable server cluster support, using the arp-mac-disparity command.

Examples

To add the IP address 10.10.10.9 with the MAC address 0010.2533.4655 into the ARP cache, and have your device respond to ARP requests for this address, use the commands:

```
awplus# configure terminal
awplus(config)# arp 10.10.10.9 0010.2355.4566 alias
```

Related commands

arp-mac-disparity

clear arp-cache

ip proxy-arp

show arp

arp log

Overview This command enables the logging of dynamic and static ARP entries in the ARP cache. The ARP cache contains mappings of device ports, VLAN IDs, and IP addresses to physical MAC addresses for hosts.

This command can display the MAC addresses in the ARP log either using the 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 22-1: 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
2018 Oct 6 06:21:01 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 add
0013.4078.3b98 (192.168.2.4)
2018 Oct 6 06:22:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 del
0013.4078.3b98 (192.168.2.4)
2018 Oct 6 06:23:26 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 add
0030.940e.136b (192.168.2.20)
2018 Oct 6 06:23:30 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Figure 22-2: 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
2018 Oct 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)
2018 Oct 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)
2018 Oct 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)
2018 Oct 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)
2018 Oct 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)
2018 Oct 6 06:28:14 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

The following table lists the parameters in 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 22-1: Parameters in the output from **show log | include ARP_LOG**

Parameter	Description
ARP_LOG	Indicates that ARP log entry information follows.
<port-number>	Indicates device port number for the ARP log entry.
<vid>	Indicates the VLAN ID for the ARP log entry.
<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.

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-reply-bc-dmac

Overview Use this command to allow processing of ARP replies that arrive with a broadcast destination MAC (ffff.ffff.ffff). This makes neighbors reachable if they send ARP responses that contain a broadcast destination MAC.

Use the **no** variant of this command to turn off processing of ARP replies that arrive with a broadcast destination MAC.

Syntax

```
arp-reply-bc-dmac
no arp-reply-bc-dmac
```

Default By default, this functionality is disabled.

Mode Interface Configuration for VLAN interfaces.

Example To allow processing of ARP replies that arrive on vlan2 with a broadcast destination MAC, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp-reply-bc-dmac
```

Related commands clear arp-cache

show arp

clear arp-cache

Overview This command deletes dynamic ARP entries from the ARP cache. You can optionally specify the IPv4 address of an ARP entry to be cleared from the ARP cache.

Syntax

```
clear arp-cache [<ip-address>]
```

Parameter	Description
<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 interface** command.

Syntax

```
debug ip packet interface {<interface-name>|all} [address
<ip-address>|verbose|hex|arp|udp|tcp|icmp]
```

```
no debug ip packet interface [<interface-name>]
```

Parameter	Description
<interface>	Specify a single Layer 3 interface name (not a range of interfaces) 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 vlan2, use the command:

```
awplus# debug ip packet interface vlan2 arp
```

To turn off IP packet interface debugging on interface vlan2, use the command:

```
awplus# no debug ip packet interface vlan2
```

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 vlan2 and IP address 192.168.2.4, use the command:

```
awplus# debug ip packet interface vlan2 address 192.168.2.4 tcp
```

Related commands

no debug all

show debugging ip dns forwarding

tcpdump

terminal monitor

undebug ip packet interface

debug ip irdp

Overview This command enables debugging of ICMP Router Discovery Protocol (IRDP) events and messages on your device. IRDP debugging is disabled by default.

The **no** variant of this command disables IRDP debugging. Negating any packet debug mode will switch detail off.

Syntax

```
debug ip irdp {event|nsm|receive|send|both|detail|all}
no debug ip irdp {event|nsm|receive|send|both|detail|all}
```

Parameter	Description
`event`	Enables debugging of IRDP events.
`nsm`	Enables debugging of IRDP processing of NSM messages.
`receive`	Enables debugging of IRDP input packet processing.
`send`	Enables debugging of IRDP output packet processing.
`both`	Enables debugging of both IRDP input and output packet processing.
`detail`	Enables detailed debugging of both IRDP input and output packet processing. Note that setting detail also sets both, so if you set **detail**, the output will show "packet debugging mode is all". Negating any packet debug mode will switch detail off.
`all`	Enables all IRDP debugging types.

Default IRDP protocol debugging is disabled by default.

Mode Privileged Exec and Global Configuration

Examples To enable IRDP input packet process debugging, use the following command:

```
awplus# debug ip irdp receive
```

To disable all IRDP debugging, use the following command:

```
awplus# no debug ip irdp all
```

Related commands

ip irdp

router ip irdp

show ip irdp

undebug ip irdp

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 a VLAN interface or a local loopback interface.

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 vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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 vlan2
awplus(config-if)# ip address 10.10.11.50/24 secondary
```

To add the IP address 10.10.11.50/24 to the local loopback interface lo, use the following commands:

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.11.50/24
```

Related commands

interface (to configure)

show ip interface

show running-config interface

ip directed-broadcast

Overview Use this command to enable flooding of directed broadcast packets into a directly connected subnet. If this command is configured on a VLAN interface, then directed broadcasts received on other VLAN interfaces, destined for the subnet on this VLAN, will be flooded to the subnet broadcast address of this VLAN.

Use the **no** variant of this command to disable **ip directed-broadcast**. When this feature is disabled using the **no** variant of this command, directed broadcasts are not forwarded.

Syntax

```
ip directed-broadcast
no ip directed-broadcast
```

Default The **ip directed-broadcast** command is disabled by default.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Usage notes IP directed-broadcast is enabled and disabled per VLAN interface. When enabled a directed broadcast packet is forwarded to an enabled VLAN interface if received on another subnet.

An IP directed broadcast is an IP packet whose destination address is a broadcast address for some IP subnet, but originates from a node that is not itself part of that destination subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is flooded as a broadcast on the destination subnet.

The **ip directed-broadcast** command controls the flooding of directed broadcasts when they reach target subnets. The command affects the final transmission of the directed broadcast on its destination subnet. It does not affect the transit unicast routing of IP directed broadcasts. If directed broadcast is enabled for an interface, incoming directed broadcast IP packets intended for the subnet assigned to the interface will be flooded as broadcasts on that subnet.

If the **no ip directed-broadcast** command is configured for an interface, directed broadcasts destined for the subnet where the interface is attached will be dropped instead of broadcast.

Examples To enable the flooding of broadcast packets out via vlan2, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip directed-broadcast
```

To disable the flooding of broadcast packets via vlan2, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip directed-broadcast
```

Related commands

ip forward-protocol udp

ip helper-address

show running-config

ip forwarding

Overview This command enables IP forwarding on your device. When enabled, your device routes IP packets.

The **no** variant of this command disables IP forwarding on your device. Even when IP forwarding is not enabled, the device can still work as an IP host; in particular, it can be managed by IP-based applications, such as SNMP, Telnet and SSH.

Syntax

```
ip forwarding
no ip forwarding
```

Default IP forwarding is enabled by default.

Mode Global Configuration

Examples To enable your device to route IP packets, use the commands:

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

To stop your device from routing IP packets, use the commands

```
awplus# configure terminal
awplus(config)# no ip forwarding
```

Related commands show ip forwarding

ip forward-protocol udp

Overview This command enables you to control which UDP broadcasts will be forwarded to the helper address(es). A UDP broadcast will only be forwarded if the destination UDP port number in the packet matches one of the port numbers specified using this command.

Refer to the IANA site (www.iana.org) for a list of assigned UDP port numbers for protocols to forward using **ip forward-protocol udp**.

Use the **no** variant of this command to remove a port number from the list of destination port numbers that are used as the criterion for deciding if a given UDP broadcast should be forwarded to the IP helper address(es).

Syntax

```
ip forward-protocol udp <port>
no ip forward-protocol udp <port>
```

Parameter	Description
<port>	UDP Port Number.

Default The **ip forward-protocol udp** command is not enabled by default.

Mode Global Configuration

Usage notes Combined with the ip helper-address command in interface mode, the **ip forward-protocol udp** command in Global Configuration mode allows control of which protocols (destination port numbers) are forwarded. The **ip forward-protocol udp** command configures protocols for forwarding, and the **ip helper-address** command configures the destination address(es).

NOTE:

*The types of UDP broadcast packets that the device will forward are ONLY those specified by the **ip forward-protocol** command(s). There are no other UDP packet types that the IP helper process forwards by default.*

NOTE:

*The **ip forward-protocol udp** command does not support BOOTP / DHCP Relay. The **ip dhcp-relay** command must be used instead. For this reason, you may not configure UDP ports 67 and 68 with the **ip forward-protocol udp** command.*

See the IP Feature Overview and Configuration Guide for more information about DNS Relay.

Examples To configure forwarding of packets on a UDP port, use the following commands:

```
awplus# configure terminal
awplus(config)# ip forward-protocol udp <port>
```

To delete a UDP port from the UDP ports that the device forwards, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip forward-protocol udp <port>
```

Related commands

ip helper-address

ip directed-broadcast

show running-config

ip gratuitous-arp-link

Overview This command sets the Gratuitous ARP time limit for all interfaces. The time limit restricts the sending of Gratuitous ARP packets to one Gratuitous ARP packet within the time in seconds.

The **no** variant of the command sets the Gratuitous ARP time limit to the default.

NOTE: *This command specifies time between sequences of Gratuitous ARP packets, and time between individual Gratuitous ARP packets occurring in a sequence, to allow legacy support for older devices and inter-operation between other devices that are not ready to receive and forward data until several seconds after linkup.*

Additionally, jitter has been applied to the delay following linkup, so Gratuitous ARP packets applicable to a given port are spread over a period of 1 second so are not all sent at once. Remaining Gratuitous ARP packets in the sequence occur after a fixed delay from the first one.

Syntax

```
ip gratuitous-arp-link <0-300>
no ip gratuitous-arp-link
```

Parameter	Description
<0-300>	Specify the minimum time between sequences of Gratuitous ARPs and the fixed time between Gratuitous ARPs occurring in a sequence, in seconds. 0 disables the sending of Gratuitous ARP packets. The default is 8 seconds.

Default The default Gratuitous ARP time limit for all interfaces is 8 seconds.

Mode Global Configuration

Usage Every switchport will send a sequence of 3 Gratuitous ARP packets to each VLAN that the switchport is a member of, whenever the switchport moves to the forwarding state. The first Gratuitous ARP packet is sent 1 second after the switchport becomes a forwarding switchport. The second and third Gratuitous ARP packets are each sent after the time period specified by the Gratuitous ARP time limit.

Additionally, the Gratuitous ARP time limit specifies the minimum time between the end of one Gratuitous ARP sequence and the start of another Gratuitous ARP sequence. When a link is flapping, the switchport's state is set to forwarding several times. The Gratuitous ARP time limit is imposed to prevent Gratuitous ARP packets from being sent undesirably often.

Examples To disable the sending of Gratuitous ARP packets, use the commands :

```
awplus# configure terminal
awplus(config)# ip gratuitous-arp-link 0
```

To restrict the sending of Gratuitous ARP packets to one every 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip gratuitous-arp-link 20
```

Related Commands show running-config

ip helper-address

Overview Use this command to add a forwarding destination address for IP Helper to enable forwarding of User Datagram Protocol (UDP) broadcasts on an interface.

Use the **no** variant of this command to disable the forwarding of broadcast packets to specific addresses.

Syntax

```
ip helper-address <ip-addr>
no ip helper-address <ip-addr>
```

Parameter	Description
<ip-addr>	Forwarding destination IP address for IP Helper.

Default The destination address for the **ip helper-address** command is not configured by default.

Mode Interface Configuration for a VLAN interface.

Usage notes Combined with the ip forward-protocol udp command in global configuration mode, the **ip helper-address** command in interface mode allows control of which protocols (destination port numbers) are forwarded. The **ip forward-protocol udp** command configures protocols for forwarding, and the **ip helper-address** command configures the destination address(es).

The destination address can be a unicast address or a subnet broadcast address. The UDP destination port is configured separately with the **ip forward-protocol udp** command. If multiple destination addresses are registered then UDP packets are forwarded to each IP address added to an IP Helper. Up to 32 destination addresses may be added using IP Helper.

The device will only forward the types of UDP broadcast packets that are specified by the **ip forward-protocol** command(s). The device does not forward any other UDP packet types by default.

The **ip helper-address** command does not support BOOTP / DHCP Relay. The service dhcp-relay command must be used instead. For this reason, you may not configure UDP ports 67 and 68 with the **ip forward-protocol** command.

See the IP Feature Overview and Configuration Guide for more information about DHCP Relay.

Examples The following example defines IPv4 address 192.168.1.100 as an IP Helper destination address to which to forward UDP broadcasts received on vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip helper-address 192.168.1.100
```

The following example removes IPv4 address 192.168.1.100 as an IP Helper destination address to which to forward UDP broadcasts received on vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip helper-address 192.168.1.100
```

Related commands

ip forward-protocol udp

ip directed-broadcast

show running-config

ip irdp

Overview This command enables ICMP Router Discovery advertising on an interface. However, the interface does not send or process Router Discovery messages until at least one IP address is configured on the interface with the ip address (IP Addressing and Protocol) command.

The **no** variant of this command disables ICMP Router Discovery advertisements on an IP interface. All transmitting and processing of Router Discovery messages ceases immediately on the interface.

Syntax

```
ip irdp
no ip irdp
```

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To enable Router Discovery advertisements on `vlan4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip irdp
```

To disable Router Discovery advertisements on `vlan4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ip irdp
```

Related commands

ip address (IP Addressing and Protocol)

show ip irdp

show ip irdp interface

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 irdp address preference

Overview When multiple routers connected to a LAN are all sending Router Discovery advertisements, hosts need to be able to choose the best router to use. Therefore the IRDP defines a preference value to place in the Router Discovery advertisements. Hosts choose the router with the highest preference value.

This command sets the preference value to include in Router Discovery advertisements sent for the specified IP address.

The **no** variant of this command sets the preference for a specific address to the default of **0**.

Syntax

```
ip irdp address <ip-address> preference <0-2147483647>
no ip irdp address <ip-address> preference
```

Parameter	Description
<ip-address>	The IP address to be advertised with the specified preference value.
<0-2147483647>	The preference value advertised. A higher number increases the preference level for this address.

Default The default preference value is 0.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To set the preference value to `3000` for the address `192.168.1.1` advertised on `vlan5`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan5
awplus(config-if)# ip irdp address 192.168.1.1 preference 3000
```

To set the preference value to the default of `0` for the address `192.168.1.1` advertised on `vlan5`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan5
awplus(config-if)# no ip irdp address 192.168.1.1 preference
```

Related commands

ip irdp

ip irdp preference

show ip irdp interface

ip irdp broadcast

Overview This command configures broadcast Router Discovery advertisements on an interface. The interface sends IRDP advertisements with the broadcast address (255.255.255.255) as the IP destination address.

The **no** variant of this command configures multicast Router Discovery advertisements on an interface. The interface sends IRDP advertisements with the all-system multicast address (224.0.0.1) as the IP destination address.

Syntax

```
ip irdp broadcast
no ip irdp broadcast
```

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To enable broadcast Router Discovery advertisements on `vlan13`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan13
awplus(config-if)# ip irdp broadcast
```

To enable multicast Router Discovery advertisements on `vlan13`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan13
awplus(config-if)# no ip irdp broadcast
```

Related commands

ip irdp

ip irdp multicast

show ip irdp interface

ip irdp holdtime

Overview This command sets the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.

The **no** variant of this command resets the holdtime back to the default of 1800 seconds.

Syntax

```
ip irdp holdtime <0-9000>
no ip irdp holdtime
```

Parameter	Description
<0-9000>	The holdtime value in seconds of addresses advertised.

Default The IRDP holdtime is set to 1800 seconds (30 minutes) by default.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To set the holdtime value of addresses advertised on `vlan2` to 4000 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip irdp holdtime 4000
```

To set the holdtime value of addresses advertised on `vlan2` back to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip irdp holdtime
```

Related commands show ip irdp interface

ip irdp lifetime

Overview This command sets the maximum length of time that hosts should consider the Router Discovery advertised addresses as valid router addresses. If you change the lifetime value, also change the **maxadvertisementinterval** and the **minadvertisementinterval** to maintain the following ratios:

This command is synonymous with the **ip irdp hostname***<0-9000>* command.

The **no** variant of this command sets the lifetime back to the default of 1800 seconds.

Syntax

```
ip irdp lifetime <0-9000>
no ip irdp lifetime
```

Parameter	Description
<0-9000>	Lifetime value in seconds of the advertised addresses.

Default The lifetime value is 1800 seconds.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To set the lifetime value to 4000 seconds for addresses advertised on `vlan6`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan6
awplus(config-if)# ip irdp lifetime 4000
```

To set the lifetime value to the default of 1800 seconds for addresses advertised on `vlan6`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan6
awplus(config-if)# no ip irdp lifetime
```

Related commands

ip irdp

ip irdp maxadvertinterval

ip irdp minadvertinterval

show ip irdp interface

ip irdp maxadvertinterval

Overview This command sets the maximum time allowed between sending router advertisements from the interface. If you change the **maxadvertisementinterval** value, also change the **lifetime** and the **minadvertisementinterval** to maintain the following ratios:

```
lifetime=3 x maxadvertisementinterval

minadvertisementinterval=0.75 x maxadvertisementinterval
```

You cannot set the maximum advertisement interval below the minimum interval. If you are lowering the maximum interval to a value below the current minimum interval, you must change the minimum value first.

The **no** variant of this command sets the **maxadvertinterval** back to the default of 600 seconds.

Syntax

```
ip irdp maxadvertinterval <4-1800>
no ip irdp maxadvertinterval
```

Parameter	Description
<4-1800>	The maximum time, in seconds, between Router Discovery advertisements.

Default The IRDP maximum advertisement interval is set to 600 seconds (10 minutes) by default.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To set the maximum interval between Router Discovery advertisements on `vlan7` to 950 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan7
awplus(config-if)# ip irdp maxadvertinterval 950
```

To set the maximum interval between advertisements on `vlan7` back to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan7
awplus(config-if)# no ip irdp maxadvertinterval
```

Related commands

ip irdp

ip irdp lifetime

ip irdp minadvertinterval

show ip irdp interface

ip irdp minadvertinterval

Overview This command sets the minimum time allowed between sending router advertisements from the interface. If you change the **minadvertisementinterval** value, also change the **lifetime** and the **maxadvertisementinterval** to maintain the following ratios:

```
lifetime=3 x maxadvertisementinterval

minadvertisementinterval=0.75 x maxadvertisementinterval
```

You cannot set the minimum advertisement interval above the maximum interval. If you are raising the minimum interval to a value above the current maximum interval, you must change the maximum value first.

The **no** variant of this command sets the **minadvertinterval** back to the default of 450 seconds.

Syntax

```
ip irdp minadvertinterval <3-1800>
no ip irdp minadvertinterval
```

Parameter	Description
<3-1800>	The minimum time between advertisements in seconds.

Default The IRDP minimum advertisement interval is set to 450 seconds (7.5 minutes) by default.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To set the minimum interval between advertisements on `vlan4` to 900 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip irdp minadvertinterval 900
```

To set the minimum interval between advertisements on `vlan4` back to the default of 450 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ip irdp minadvertinterval
```

Related commands

ip irdp

ip irdp lifetime

ip irdp maxadvertinterval

show ip irdp interface

ip irdp multicast

Overview This command configures multicast Router Discovery advertisements on an interface. The interface sends IRDP advertisements with the all-system multicast address (224.0.0.1) as the IP destination address.

The **no** variant of this command configures broadcast Router Discovery advertisements on an interface. The interface sends IRDP advertisements with the broadcast address (255.255.255.255) as the IP destination address.

The multicast address is the default IP destination address for Router Discovery advertisements.

Syntax

```
ip irdp multicast
no ip irdp multicast
```

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To enable multicast Router Discovery advertisements on `vlan5`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan5
awplus(config-if)# ip irdp multicast
```

To enable broadcast Router Discovery advertisements on `vlan5`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan5
awplus(config-if)# no ip irdp multicast
```

Related commands

ip irdp

ip irdp broadcast

show ip irdp interface

ip irdp preference

Overview When multiple routers connected to a LAN are all sending Router Discovery advertisements, hosts need to be able to choose the best router to use. Therefore the IRDP defines a preference value to place in the Router Discovery advertisements. Hosts choose the router with the highest preference value.

This command sets the preference value to include in Router Discovery advertisements sent for the specified interface.

When this command is used, all IP addresses on the interface are assigned the same preference value, except the addresses that have specific preference value assignment using the command ip irdp address preference.

The **no** variant of this command sets the preference value to the default of 0.

Syntax

```
ip irdp preference <0-2147483647>
no ip irdp preference
```

Parameter	Description
<0-2147483647>	The preference value for the interface. A higher number increases the preference level for addresses on the specific interface.

Default The default preference value is 0.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To set the preference of addresses advertised on `vlan6` to `500`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan6
awplus(config-if)# ip irdp preference 500
```

To set the preference value for addresses on `vlan6` back to the default of `0`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan6
awplus(config-if)# no ip irdp preference
```

Related commands ip irdp

ip irdp address preference

show ip irdp interface

ip limited-local-proxy-arp

Overview Use this command to enable local proxy ARP, but only for a specified set of IP addresses. This makes the device respond to ARP requests for those IP addresses when the addresses are reachable via the interface you are configuring.

To specify the IP addresses, use the command local-proxy-arp.

Use the **no** variant of this command to disable limited local proxy ARP. This stops your device from intercepting and responding to ARP requests for the specified hosts. This allows the hosts to use MAC address resolution to communicate directly with one another.

Syntax

```
ip limited-local-proxy-arp
no ip limited-local-proxy-arp
```

Default Limited local proxy ARP is disabled by default.

Mode Interface Configuration

Usage This command allows you to stop MAC address resolution for specified hosts. Limited local proxy ARP works by intercepting ARP requests for the specified hosts and responding with your device's own MAC address details instead of the destination host's details. This stops hosts from learning the MAC address of the other hosts through ARP requests.

Limited local proxy ARP ensures that the specified devices cannot send traffic that bypasses Layer 3 routing on your device. This gives you control over which hosts may communicate with one another.

Example To enable limited local proxy ARP, so that the device makes ARP responses to ARP requests for specified addresses, when the ARP requests are received on VLAN2 and the addresses are routed out VLAN2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip limited-local-proxy-arp
```

Related commands ip local-proxy-arp

local-proxy-arp

ip local-proxy-arp

Overview This command allows you to stop MAC address resolution between hosts within a private VLAN edge interface. Local Proxy ARP works by intercepting ARP requests between hosts within a subnet and responding with your device's own MAC address details instead of the destination host's details. This stops hosts from learning the MAC address of other hosts within its subnet through ARP requests.

Local Proxy ARP ensures that devices within a subnet cannot send traffic that bypasses Layer 3 routing on your device. This lets you monitor and filter traffic between hosts in the same subnet, and enables you to have control over which hosts may communicate with one another.

When Local Proxy ARP is operating on an interface, your device does not generate or forward any ICMP-Redirect messages on that interface. This command does not enable proxy ARP on the interface; see the ip proxy-arp command for more information on enabling proxy ARP.

The **no** variant of this command disables Local Proxy ARP to stop your device from intercepting and responding to ARP requests between hosts within a subnet. This allows the hosts to use MAC address resolution to communicate directly with one another. Local Proxy ARP is disabled by default.

Syntax

```
ip local-proxy-arp
no ip local-proxy-arp
```

Default Local proxy ARP is disabled by default

Mode Interface Configuration for VLAN interfaces.

Examples To enable your device to apply Local Proxy ARP on the interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip local-proxy-arp
```

To disable your device to apply Local Proxy ARP on the interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip local-proxy-arp
```

Related commands ip proxy-arp

show arp

show running-config

ip proxy-arp

Overview This command enables Proxy ARP responses to ARP requests on an interface. When enabled, your device intercepts ARP broadcast packets and substitutes its own physical address for that of the remote host. By responding to the ARP request, your device ensures that subsequent packets from the local host are directed to its physical address, and it can then forward these to the remote host.

Your device responds only when it has a specific route to the address being requested, excluding the interface route that the ARP request arrived from. It ignores all other ARP requests. See the ip local-proxy-arp command about enabling your device to respond to other ARP messages.

The **no** variant of this command disables Proxy ARP responses on an interface. Proxy ARP is disabled by default.

Syntax

```
ip proxy-arp
no ip proxy-arp
```

Default Proxy ARP is disabled by default.

Mode Interface Configuration for VLAN interfaces.

Examples To enable your device to Proxy ARP on the interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip proxy-arp
```

To disable your device to Proxy ARP on the interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip proxy-arp
```

Related commands

arp

ip local-proxy-arp

show arp

show running-config

ip redirects

Overview This command enables the device to send ICMP redirects on one or more interfaces.

Use the **no** variant of this command to stop the device from sending ICMP redirects on one or more interfaces.

Syntax

```
ip redirects
no ip redirects
```

Default ICMP redirects are disabled by default.

Mode Interface Configuration for a VLAN interface.

Usage notes ICMP redirect messages are used to notify hosts that a better route is available to a destination.

ICMP redirects are used when a packet is routed into the device on the same interface that the packet is routed out of the device. ICMP redirects are only sent to packet sources that are directly connected to the device.

Examples To enable the device to send ICMP redirects on interface vlan2, use the following commands:

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

To stop the device from sending ICMP redirects on interface vlan2, use the following commands:

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

ip tcp synack-retries

Overview Use this command to specify how many times the switch will retry sending a SYN ACK for a TCP connection for which it has received a SYN but not an ACK. Such connections are called half-open TCP connections. This command allows you to influence how long half-open TCP connections take to time out.

Use the **no** variant of this command to return to the default setting of 5 retries.

Syntax

```
ip tcp synack-retries <0-255>
no ip tcp synack-retries
```

Parameter	Description
<0-255>	Number of times to retry sending the SYN ACK

Default 5 retries

Mode Global Configuration

Usage notes The following table shows the approximate correlation between the number of retries and the time half-open TCP connections take to time out.

Number of retries	Approximate lower bound for the timeout
0 retries	1 second
1 retry	3 seconds
2 retries	7 seconds
3 retries	15 seconds
4 retries	31 seconds
5 retries	63 seconds

Example To retry twice, which leads to a timeout of approximately 7 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip tcp synack-retries 2
```

Related commands show running-config

Command changes Version 5.4.7-0.2: command added

ip 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 22-2: 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 22-2: 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
```

local-proxy-arp

Overview Use this command to specify an IP subnet for use with limited local proxy ARP. When limited local proxy ARP is enabled with the command ip limited-local-proxy-arp, the device will respond to ARP requests for addresses in that subnet.

Use the **no** variant of this command to stop specifying a subnet for use with limited local proxy ARP.

Syntax

```
local-proxy-arp [<ip-add/mask>]
no local-proxy-arp [<ip-add/mask>]
```

Parameter	Description
<ip-add/mask>	The IP subnet to use with limited local proxy ARP, in dotted decimal format (A.B.C.D/M). To specify a single IP address, use a 32-bit mask.

Default No subnets are specified for use with limited local proxy ARP.

Mode Global Configuration

Example To specify limited local proxy ARP for the address 172.22.0.3, use the following commands:

```
awplus# configure terminal
awplus(config)# local-proxy-arp 172.22.0.3/32
```

Related commands ip limited-local-proxy-arp

optimistic-nd

Overview Use this command to enable the optimistic neighbor discovery feature for both IPv4 and IPv6.

Use the **no** variant of this command to disable the optimistic neighbor discovery feature.

Syntax

```
optimistic-nd
no optimistic-nd
```

Default The optimistic neighbor discovery feature is enabled by default.

Mode Interface Configuration for a VLAN interface.

Usage notes The optimistic neighbor discovery feature allows the device, after learning an IPv4 or IPv6 neighbor, to refresh the neighbor before the neighbor is deleted from the hardware L3 switching table. The device puts the neighbor entry into the ‘stale’ state in the software switching table if is it not refreshed, then the 'stale' neighbors are deleted from the hardware L3 switching table.

The optimistic neighbor discovery feature enables the device to sustain L3 traffic switching to a neighbor without interruption. Without the optimistic neighbor discovery feature enabled L3 traffic is interrupted when a neighbor is ‘stale’ and is then deleted from the L3 switching table.

If a neighbor receiving optimistic neighbor solicitations does not answer optimistic neighbor solicitations with neighbor advertisements, then the neighbor will be put into the ‘stale’ state, and subsequently deleted from both the software and the hardware L3 switching tables.

Examples To enable the optimistic neighbor discovery feature on vlan2, use the following commands:

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

To disable the optimistic neighbor discovery feature on vlan2, use the following commands:

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

Related commands show running-config

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
```

router ip irdp

Overview This command globally enables ICMP Router Discovery (IRDP) advertisements on your device. However, your device does not send or process IRDP messages until at least one interface is configured to use IP and has had IRDP enabled on the interface with the ip irdp command.

The **no** variant of this command globally disables IRDP advertisements on the device. All interfaces immediately stop transmitting and processing Router Discovery messages.

Syntax

```
router ip irdp
no router ip irdp
```

Mode Global Configuration

Examples To enable Router Discovery advertisements on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# router ip irdp
```

To disable Router Discovery advertisements on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# no router ip irdp
```

Related commands ip irdp

show ip irdp

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 22-3: Example output from the **show arp** command

```
awplus#show arp
IP Address       LL Address        Interface  Port          Type
192.168.27.10    192.168.4.1       vlan1      port1.0.1     dynamic
192.168.27.100   0000.daaf.cd24    vlan1      port1.0.2     dynamic
192.168.1.100    192.168.20.1      vlan2      port1.0.3     static
```

Table 23: 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 debugging ip packet

Overview Use this command to see what debugging is turned on for IP interfaces. IP interface debugging is set using the **debug ip packet interface** command.

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

Syntax

```
show debugging ip packet
```

Mode User Exec and Privileged Exec

Example To display the IP interface debugging status when the terminal monitor is off, use the commands:

```
awplus# terminal no monitor
awplus# show debugging ip packet
```

Output Figure 22-4: Example output from the **show debugging ip packet** command with **terminal monitor** off

```
awplus#terminal no monitor
awplus#show debugging ip packet
IP debugging status:
interface all tcp (stopped)
interface vlan1 arp verbose (stopped)
```

Example To display the IP interface debugging status when the terminal monitor is on, use the commands:

```
awplus# terminal monitor
awplus# show debugging ip packet
```

Output Figure 22-5: Example output from the **show debugging ip packet** command with **terminal monitor** on

```
awplus#terminal monitor
awplus#show debugging ip packet
IP debugging status:
interface all tcp (running)
interface vlan1 arp verbose (running)
```

Related commands debug ip packet interface

terminal monitor

show ip flooding-nexthops

Overview Use this command to display the static and dynamic ARP entries in the ARP cache that flood packets to multiple ports.

Syntax
```
show ip flooding-nexthops
```

Mode User Exec and Privileged Exec

Example To display all of the flooding nexthop entries in the ARP cache, use the command:

```
awplus# show ip flooding-nexthops
```

Output Figure 22-6: Example output from **show ip flooding-nexthops**

```
awplus#show ip flooding-nexthops
IP Address      MAC Address     Interface         Flooding Mode    Type
11.11.11.10     0300.0000.0011  vlan1             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 22-7: Example output from the **show ip forwarding** command

```
awplus#show ip forwarding
IP forwarding is on
```

Related commands ip forwarding

show ip interface

Overview Use this command to display information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

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

Syntax

```
show ip interface [<interface-list>] [brief]
```

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: • a VLAN (e.g. vlan2) • the loopback interface (lo) • a continuous range of interfaces separated by a hyphen (e.g. vlan10-20) • a comma-separated list (e.g. vlan1,vlan10-20). Do not mix interface types in a list. The specified interfaces must exist.

Mode User Exec and Privileged Exec

Examples To show brief information for the assigned IP address for interface vlan2 use the command:

```
awplus# show ip interface vlan2 brief
```

Output Figure 22-8: Example output from the **show ip interface brief** command

```
Interface              IP-Address      Status          Protocol
port1.0.1              unassigned      admin up        down
...
vlan1                  192.168.1.1     admin up        running
...
```

show ip irdp

Overview This command displays whether IRDP is globally enabled on your device, and the status of the debugging modes.

If the **debug ip irdp** command has been set with the **detail** parameter then the **both** parameter is also set and the output will show "packet debugging mode is all".

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

Syntax

```
show ip irdp
```

Mode User Exec and Privileged Exec

Example To display global IRDP configuration, use the command:

```
awplus# show ip irdp
```

Output Figure 22-9: Example output from the **show ip irdp** command

```
IRDP is enabled
  event debugging is disabled
  nsm debugging is disabled
  packet debugging mode is disabled
```

Figure 22-10: Example output from the **show ip irdp** command with **debug ip irdp detail** set

```
IRDP is enabled
  event debugging is disabled
  nsm debugging is disabled
  packet debugging mode is all
```

Figure 22-11: Example output from the **show ip irdp** command with **debug ip irdp both** set

```
IRDP is enabled
  event debugging is disabled
  nsm debugging is disabled
  packet debugging mode is both
```

Related commands debug ip irdp

router ip irdp

show ip irdp interface

Overview This command displays the configuration of IRDP on all interfaces, or for a specified interface.

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

Syntax

```
show ip irdp interface [<interface-name>]
```

Parameter	Description
<interface-name>	Displays the interface status and configuration details of the specified interface.

Mode User Exec and Privileged Exec

Example To display the IRDP configuration for `vlan4`, use the command:

```
awplus# show ip irdp interface vlan4
```

Output Figure 22-12: Example output from the **show ip irdp interface** command

```
vlan13 is up, line protocol is up
ICMP Router Discovery Protocol
  Sending mode          multicast
  Router Lifetime       1350 seconds
  Default Preference    0
  Min Adv Interval      450 seconds
  Max Adv Interval      600 seconds
  Next advertisement in 551 seconds
  Non default prefix preferences
     192.168.1.1        preference     25000

  In packets                  0                Out packets                  3
  In bad packets              0                Out bad packets              0
  In good packets             0                Out good packets             3
  In ignored packets          0
```

Table 24: Parameters in the output of the **show ip irdp interface** command

Parameter	Description
`Sending mode`	Whether this interface is sending broadcast or multicast router advertisements. This means the destination IP address of router advertisements will be either the multicast address 224.0.0.1, or the broadcast address 255.255.255.255.
`Router Lifetime`	The lifetime value set for router advertisements sent from this interface. This is the maximum time that other devices should treat the advertised address as valid.
`Default Preference`	The preference value for IP addresses as default router addresses, relative to other router addresses on the same subnet. This preference value is used for all IP addresses on this interface, except for those listed under the heading “non default prefix preferences”.
`Min Adv Interval`	Minimum time allowed between sending router advertisements from this interface.
`Max Adv Interval`	Maximum time allowed between sending router advertisements from this interface.
`Non default prefix preferences`	List of the IP addresses on this interface that have been set with a specific router preference value. These addresses use the preference value listed beside them, rather than the interface’s default preference value.
`In packets`	The total number of packets received by IRDP on this interface. IRDP processes all ICMP packets received on this interface.
`Out packets`	The number of packets sent by IRDP on this interface.
`In bad packets`	The number of packets received by IRDP that it has discarded because they do not conform or corrupted.
`Out bad packets`	The number of packets that IRDP generated but failed to send to the network layer.
`In good packets`	The number of packets received and processed by IRDP.
`Out good packets`	The number of packets generated and successfully sent by IRDP.
`In ignored packets`	The number of incoming packets ignored, like ICMP packets other than IRDP.

Related commands

ip irdp

show ip irdp

show ip sockets

Overview Use this command to display information about the IP or TCP sockets that are present on the device. It includes TCP and UDP listen sockets, and displays the associated IP address and port.

The information displayed for established TCP sessions includes the remote IP address, port, and session state. Raw IP protocol listen socket information is also displayed for protocols such as VRRP and ICMP6, which are configured to receive IP packets with the associated protocol number.

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

Syntax

```
show ip sockets
```

Mode Privileged Exec

Usage notes Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

Note that this command does not display sockets that are used internally for exchanging data between the various processes that exist on the device and are involved in its operation and management. It only displays sockets that are present for the purposes of communicating with other external devices.

Example To display IP sockets currently present on the device, use the command:

```
awplus# show ip sockets
```

Output Figure 22-13: 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 22-1: 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 (either IPv4 or IPv6) 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 22-1: 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 or :: for IPv6. 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: or ::: for IPv4 and IPv6, respectively.

`State`	This column shows the state of the socket. For TCP sockets this shows the state of the TCP state machine. For UDP sockets this column is blank. For raw sockets it contains the IP protocol number. The possible TCP states are:
	`LISTEN`
	`SYN-SENT`
	`SYN-RECEIVED`
	`ESTABLISHED`
	`FIN-WAIT-1`
	`FIN-WAIT-2`
	`CLOSE-WAIT`
	`CLOSING`
	`LAST-ACK`
	`TIME-WAIT`
	`CLOSED`
	RFC793 contains the TCP state machine diagram with Section 3.2 describing each of the states.

show ip traffic

Overview Use this command to display statistics regarding IP traffic sent and received by all interfaces on the device, showing totals for IP and IPv6 and then broken down into sub-categories such as TCP, UDP, ICMP and their IPv6 equivalents when appropriate.

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

Syntax

```
show ip traffic
```

Mode Privileged Exec

Example To display IP traffic statistics, use the command:

```
awplus# show ip traffic
```

Output Figure 22-14: Example output from the **show ip traffic** command

```
awplus#show ip traffic
IP:
    168475 packets received
    168475 delivered
    208099 sent
    35 dropped due to missing route
    22646409 bytes received
    126783216 bytes sent
    InCsumErrors 0
    InNoECTPkts 168475
    InECT1Pkts 0
    InECT0Pkts 0
    InCEPkts 0
    In107 Destination Unreachable
    Out11 Destination Unreachable
IPv6:
    14 packets received
    14 received packets delivered
    18 packets transmitted
...
ICMP6:
    4 messages sent
...
UDP6:
    Udp6RcvbufErrors 0
...
UDPLite6:
    UdpLite6RcvbufErrors 0
...
```

```
TCP:
    8 remote connections established
...
UDP:
    79797 datagrams received
...
UDPLite:
    InCsumErrors 0
...
```

tcpdump

Overview Use this command to start a tcpdump, which gives the same output as the Unix-like **tcpdump** command to display TCP/IP traffic. Press `<ctrl> + c` to stop a running tcpdump.

Syntax `tcpdump <line>`

Parameter	Description
<line>	Specify the dump options. For more information on the options for this placeholder see http://www.tcpdump.org/tcpdump_man.html

Mode Privileged Exec

Example To start a tcpdump running to capture IP packets, enter the command:

```
awplus# tcpdump ip
```

Output Figure 22-15: 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.

undebug ip irdp

Overview This command applies the functionality of the no debug ip irdp command.

23 Domain Name Service (DNS) Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure Domain Name Service (DNS) features, including the following:

- DNS client
- DNS forwarding (DNS relay)

For more information about DNS for Switches, see the Domain Name System (DNS) for AlliedWare Plus Switches Feature Overview and Configuration Guide

Command List

- "clear ip dns forwarding cache" on page 900
- "debug ip dns forwarding" on page 901
- "ip dns forwarding" on page 902
- "ip dns forwarding cache" on page 903
- "ip dns forwarding dead-time" on page 904
- "ip dns forwarding retry" on page 905
- "ip dns forwarding source-interface" on page 906
- "ip dns forwarding timeout" on page 907
- "ip domain-list" on page 908
- "ip domain-lookup" on page 909
- "ip domain-name" on page 911
- "ip name-server" on page 912
- "ip name-server preferred-order" on page 914
- "show debugging ip dns forwarding" on page 915
- "show hosts" on page 916
- "show ip dns forwarding" on page 917

- "show ip dns forwarding cache" on page 918
- "show ip dns forwarding server" on page 919
- "show ip domain-list" on page 920
- "show ip domain-name" on page 921
- "show ip name-server" on page 922

clear ip dns forwarding cache

Overview Use this command to clear the DNS Relay name resolver cache.

Syntax

```
clear ip dns forwarding cache
```

Mode Privileged Exec

Examples To clear all cached data, use the command:

```
awplus# clear ip dns forwarding cache
```

Related commands ip dns forwarding cache

debug ip dns forwarding

Overview Use this command to enable DNS Relay debugging.

Use the **no** variant of this command to disable DNS Relay debugging.

Syntax

```
debug ip dns forwarding
no debug ip dns forwarding
```

Default DNS Relay debugging is disabled by default.

Mode Privileged Exec

Examples To enable DNS forwarding debugging, use the commands:

```
awplus# debug ip dns forwarding
```

To disable DNS forwarding debugging, use the commands:

```
awplus# no debug ip dns forwarding
```

Related commands ip dns forwarding

show debugging ip dns forwarding

ip dns forwarding

Overview Use this command to enable DNS Relay, the forwarding of incoming DNS queries for IP hostname-to-address translation.

Use the **no** variant of this command to disable the forwarding of incoming DNS queries for IP hostname-to-address translation.

Syntax

```
ip dns forwarding
no ip dns forwarding
```

Default The forwarding of incoming DNS query packets is disabled by default.

Mode Global Configuration

Usage notes DNS Relay is independent of the configuration of ip domain-lookup (which is enabled by default). If ip domain-lookup is disabled, but DNS Relay is enabled, the router will continue to forward DNS queries by hosts in the network to its configured name-servers.

See the ip dns forwarding dead-time command used with this command.

Examples To enable the forwarding of incoming DNS query packets, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding
```

To disable the forwarding of incoming DNS query packets, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding
```

Related commands

clear ip dns forwarding cache

debug ip dns forwarding

ip dns forwarding cache

ip dns forwarding dead-time

ip dns forwarding retry

ip dns forwarding source-interface

ip dns forwarding timeout

ip domain-lookup

ip name-server

show ip dns forwarding

show ip dns forwarding cache

show ip dns forwarding server

ip dns forwarding cache

Overview Use this command to set the DNS Relay name resolver cache size and cache entry lifetime period. The DNS Relay name resolver cache stores the mappings between domain names and IP addresses.

Use the **no** variant of this command to set the default DNS Relay name resolver cache size and cache entry lifetime period.

Note that the lifetime period of the cache entry can be overwritten by the time-out period of the DNS reply from the DNS server if the time-out period of the DNS reply from the DNS server is smaller than the configured time-out period. The time-out period of the cache entry will only be used when the time-out period of the DNS reply from the DNS server is bigger than the time-out period configured on the device.

Syntax

```
ip dns forwarding cache [size <0-10000>] [timeout <60-3600>]
no ip dns forwarding cache [size|timeout]
```

Parameter	Description
<0-10000>	Number of entries in the DNS Relay name resolver cache.
<60-3600>	Timeout value in seconds.

Default The default cache size is 0 (no entries) and the default lifetime is 1800 seconds.

Mode Global Configuration

Examples To set the cache size to `10` entries and the lifetime to `500` seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding cache size 10 time 500
```

To set the cache size to the default, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding cache size
```

Related commands

clear ip dns forwarding cache

debug ip dns forwarding

ip dns forwarding

show ip dns forwarding

show ip dns forwarding cache

Command changes Version 5.4.8-1.1: maximum cache limit increased to 10000

ip dns forwarding dead-time

Overview Use this command to set the time period in seconds when the device stops sending any DNS requests to an unresponsive server and all retries set using ip dns forwarding retry are used. This time period is the DNS forwarding dead-time. The device stops sending DNS requests at the DNS forwarding dead-time configured and when all of the retries are used.

Use the **no** variant of this command to restore the default DNS forwarding dead-time value of 3600 seconds.

Syntax

```
ip dns forwarding dead-time <60-43200>
no ip dns forwarding retry
```

Parameter	Description
<60-43200>	Set the DNS forwarding dead-time in seconds. At the dead-time set, the switch stops sending DNS requests to an unresponsive server.

Default The default time to stop sending DNS requests to an unresponsive server is 3600 seconds.

Mode Global Configuration

Usage notes See the ip dns forwarding retry command used with this command.

Examples To set the DNS forwarding retry count to 50 and to set the DNS forwarding dead-time to 1800 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dead-time 1800
awplus(config)# ip dns forwarding retry 50
```

To reset the DNS retry count to the default of 2 and the DNS forwarding dead-time to the default of 3600, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dead-time
awplus(config)# no ip dns forwarding retry
```

Related commands

debug ip dns forwarding

ip dns forwarding

ip dns forwarding retry

show ip dns forwarding

show ip dns forwarding server

ip dns forwarding retry

Overview Use this command to set the number of times DNS Relay will retry to forward DNS queries. The device stops sending DNS requests to an unresponsive server at the time set using the ip dns forwarding dead-time command and when all of the retries are used.

Use the **no** variant of this command to set the number of retries to the default of 2.

Syntax

```
ip dns forwarding retry <0-100>
no ip dns forwarding retry
```

Parameter	Description
<0-100>	Set the number of times DNS Relay will retry to forward a DNS query.

Default The default number of retries is 2 DNS requests to an unresponsive server.

Mode Global Configuration

Usage notes See the ip dns forwarding dead-time command used with this command.

Examples To set the DNS forwarding retry count to `50` and to set the DNS forwarding dead-time to `1800` seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding retry 50
awplus(config)# ip dns forwarding dead-time 1800
```

To reset the DNS retry count to the default of `2` and the DNS forwarding dead-time to the default of `3600` seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding retry
awplus(config)# no ip dns forwarding dead-time
```

Related commands

debug ip dns forwarding

ip dns forwarding

ip dns forwarding dead-time

show ip dns forwarding

ip dns forwarding source-interface

Overview Use this command to set the interface to use for forwarding and receiving DNS queries.

Use the **no** variant of this command to unset the interface used for forwarding and receiving DNS queries.

Syntax

```
ip dns forwarding source-interface <interface-name>
no ip dns forwarding source-interface
```

Parameter	Description
<interface-name>	An alphanumeric string that is the interface name.

Default The default is that no interface is set and the device selects the appropriate source IP address automatically.

Mode Global Configuration

Examples To set `vlan1` as the source interface for relayed DNS queries, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding source-interface vlan1
```

To clear the source interface for relayed DNS queries, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding source-interface
```

Related commands

debug ip dns forwarding

ip dns forwarding

show ip dns forwarding

ip dns forwarding timeout

Overview Use this command to set the time period for the DNS Relay to wait for a DNS response.

Use the **no** variant of this command to set the time period to wait for a DNS response to the default of 3 seconds.

Syntax

```
ip dns forwarding timeout <0-3600>
no ip dns forwarding timeout
```

Parameter	Description
<0-3600>	Timeout value in seconds.

Default The default timeout value is 3 seconds.

Mode Global Configuration

Examples To set the timeout value to 12 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding timeout 12
```

To set the timeout value to the default of 3 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding timeout
```

Related commands

debug ip dns forwarding

ip dns forwarding

show ip dns forwarding

ip domain-list

Overview This command adds a domain to the DNS list. Domains are appended to incomplete host names in DNS requests. Each domain in this list is tried in turn in DNS lookups. This list is ordered so that the first entry you create is checked first.

The **no** variant of this command deletes a domain from the list.

Syntax

```
ip domain-list <domain-name>
no ip domain-list <domain-name>
```

Parameter	Description
<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.

It is possible to configure the DNS client to use the DNS relay to resolve domain lookups originating from the device itself. This configuration may be preferred, as the DNS relay provides additional functionality that is not available in the DNS client, such as caching, a configurable timeout length, and other options.

The **no** variant of this command disables the DNS client. The client will not attempt to resolve domain names. You must use IP addresses to specify hosts in commands.

Syntax

```
ip domain-lookup [via-relay]
no ip domain-lookup
```

Parameter	Description
via-relay	Perform resolution via DNS relay

Mode Global Configuration

Usage notes The client is enabled by default. However, it does not attempt DNS inquiries unless there is a DNS server configured.

Examples To enable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-lookup
```

To configure the DNS client to perform resolution via the DNS relay, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-lookup via-relay
awplus(config)# ip dns forwarding
```

To disable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip domain-lookup
```

Related commands

ip domain-list

ip domain-name

ip name-server

show hosts

show ip name-server

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>
```

Parameter	Description
<domain-name>	Domain string, for example “company.com”.

Mode Global Configuration

Usage notes If there are no domains in the DNS list (created using the ip domain-list command) then your device uses the domain specified with this command. If any domain exists in the DNS list, then the device does not use the domain configured with this command.

When your device is using its DHCP client for an interface, it can receive Option 15 from the DHCP server. This option replaces the domain name set with this command.

Example To configure the domain name, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-name company.com
```

Related commands

ip domain-list

show ip domain-list

show ip domain-name

ip name-server

Overview Use this command to add IPv4 or IPv6 DNS server addresses. The DNS client on your device sends DNS queries to IP addresses in this list when trying to resolve a host name. Host names cannot be resolved until you have added at least one server to this list. A maximum of three name servers can be added to this list.

The **no** variant of this command removes the specified DNS name-server address.

Syntax

```
ip name-server <ip-addr>
no ip name-server <ip-addr>
```

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 domain-list

ip domain-lookup

ip domain-name

show ip dns forwarding cache

show ip name-server

Command changes

Version 5.4.6-2.1: VRF-lite support added to AR-series devices.

ip name-server preferred-order

Overview Use this command to choose between using statically-configured DNS servers or dynamically-learned DNS servers.

Use the **no** variant of this command to set the DNS servers back to the default setting of dynamic.

Syntax

```
ip name-server preferred-order {dynamic|static}
no ip name-server preferred-order
```

Parameter	Description
`dynamic`	Use dynamically learned DNS servers first.
`static`	Use statically configured DNS servers first.

Default dynamic

Mode Global Configuration

Usage notes This command is used to choose which DNS server set to use first. Select either the **dynamic** or **static** parameter.

Examples To configure the preference to use static servers first, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server preferred-order static
```

To configure the preference to use dynamically-learned servers first, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server preferred-order dynamic
```

or

```
awplus# configure terminal
awplus(config)# no ip name-server preferred-order
```

Related commands

ip address dhcp

ip name-server

ipv6 address dhcp

show ip name-server

Command changes Version 5.4.9-0.1: command added

show debugging ip dns forwarding

Overview Use this command to see what debugging is turned on for DNS Relay. DNS Relay debugging is set using the **debug ip dns forwarding** command.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show debugging ip dns forwarding
```

Mode User Exec and Privileged Exec

Example To display the DNS Relay debugging status, use the command:

```
awplus# show debugging ip dns forwarding
```

Output Figure 23-1: Example output from the **show debugging ip dns forwarding** command:

```
awplus#show debugging ip dns forwarding

DNS Relay debugging status:
  debugging is on
```

Related commands debug ip dns forwarding

show hosts

Overview This command shows the default domain, domain list, and name servers configured on your device.

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

Syntax

```
show hosts
```

Mode User Exec and Privileged Exec

Example To display the default domain, use the command:

```
awplus# show hosts
```

Output Figure 23-2: 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 23-3: Example output from the **show hosts** command when **ip domain-lookup** is configured

```
awplus#show hosts

Default domain is mycompany.com
Domain list: company.com
Name/address lookup uses domain service
Name servers are 10.10.0.2 10.10.0.88
```

Figure 23-4: Example output from the **show hosts** command when **ip domain-lookup via-relay** is configured

```
awplus#show hosts

Default domain is mycompany.com
Domain list: company.com
Name/address lookup uses domain relay service
Name servers are 10.10.0.2 10.10.0.88
```

Related commands

ip domain-list

ip domain-lookup

ip domain-name

ip name-server

show ip dns forwarding

Overview Use this command to display the DNS Relay status.

Syntax

```
show ip dns forwarding
```

Mode User Exec and Privileged Exec

Examples To display the DNS Relay status, use the command:

```
awplus# show ip dns forwarding
```

Output Figure 23-5: Example output from the **show ip dns forwarding** command

```
awplus#show ip dns forwarding

Max-Retry       : 2
Timeout         : 3 second(s)
Dead-Time       : 3600 second(s)
Source-Interface: not specified
DNS Cache       : disabled
```

Related commands ip dns forwarding

show ip dns forwarding cache

Overview Use this command to display the DNS Relay name resolver cache.

Syntax

```
show ip dns forwarding cache
```

Mode User Exec and Privileged Exec

Example To display the DNS Relay name resolver cache, use the command:

```
awplus# show ip dns forwarding cache
```

Output Figure 23-6: Example output from the **show ip dns forwarding cache** command

```
awplus#show ip dns forwarding cache
IPv4 addresses in cache:     3
IPv6 addresses in cache:     0
Cache size: 1000
Host                                    Address                 Expires Flags
www.example.com                         172.16.1.1.                 180
mail.example.com                        www.example.com             180 CNAME
www.example.com                         172.16.1.1.                 180 REVERSE
mail.example.com                        172.16.1.5.                 180
```

Related commands

ip dns forwarding cache

ip name-server

show ip dns forwarding server

Overview Use this command to display the status of DNS forwarding name servers.

Syntax

```
show ip dns forwarding server
```

Parameter	Description
`forwarding server`	Display information about the DNS forwarding name servers.

Mode User Exec and Privileged Exec

Examples To display the status of DNS Relay name servers, use the command:

```
awplus# show ip dns forwarding server
```

Output Figure 23-7: Example output from the **show ip dns forwarding server** command

```
awplus#show ip dns forwarding server

Servers            Forwards      Fails     Dead-Time
172.16.1.1              12          0       active
172.16.1.2               6          3         3900
```

Related commands ip dns forwarding

ip dns forwarding dead-time

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 23-8: 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 23-9: 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 23-10: 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

24 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 925
- "ipv6 address" on page 926
- "ipv6 address autoconfig" on page 928
- "ipv6 address suffix" on page 930
- "ipv6 enable" on page 931
- "ipv6 eui64-linklocal" on page 933
- "ipv6 forwarding" on page 934
- "ipv6 icmp error-interval" on page 935
- "ipv6 multicast forward-slow-path-packet" on page 936
- "ipv6 nd accept-ra-default-routes" on page 937
- "ipv6 nd accept-ra-pinfo" on page 938
- "ipv6 nd current-hoplimit" on page 939
- "ipv6 nd dns search-list" on page 940
- "ipv6 nd dns-server" on page 941
- "ipv6 nd managed-config-flag" on page 942
- "ipv6 nd minimum-ra-interval" on page 943
- "ipv6 nd other-config-flag" on page 944
- "ipv6 nd prefix" on page 945
- "ipv6 nd ra-interval" on page 947

- "ipv6 nd ra-lifetime" on page 948
- "ipv6 nd raguard" on page 949
- "ipv6 nd reachable-time" on page 951
- "ipv6 nd retransmission-time" on page 952
- "ipv6 nd route-information" on page 953
- "ipv6 nd router-preference" on page 954
- "ipv6 nd suppress-ra" on page 955
- "ipv6 neighbor" on page 956
- "ipv6 opportunistic-nd" on page 957
- "ipv6 route" on page 958
- "ipv6 unreachables" on page 959
- "optimistic-nd" on page 960
- "ping ipv6" on page 961
- "show ipv6 forwarding" on page 963
- "show ipv6 interface" on page 964
- "show ipv6 neighbors" on page 965
- "show ipv6 route" on page 966
- "show ipv6 route summary" on page 968
- "traceroute ipv6" on page 969

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 ipv6 neighbor

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. Note that your switch will not accept prefix lengths greater than 64.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Usage notes Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them. See the ipv6 enable command for more information.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the ipv6 enable command then it will not be removed using a **no ipv6 address** command.

Examples To assign the IPv6 address 2001:0db8::a2/64 to the VLAN interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the VLAN interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

Related commands

ipv6 address autoconfig

ipv6 address dhcp

ipv6 enable

ipv6 eui64-linklocal

show running-config

show ipv6 interface

show ipv6 route

ipv6 address autoconfig

Overview Use this command to enable IPv6 stateless address autoconfiguration (SLAAC) for an interface. This configures an IPv6 address on an interface derived from the MAC address on the interface.

Use the **no** variant of this command to disable IPv6 SLAAC on an interface. Note that if no global addresses are left after removing all IPv6 autoconfigured addresses then IPv6 is disabled.

Syntax

```
ipv6 address autoconfig
no ipv6 address autoconfig
```

Mode Interface Configuration for a VLAN interface or a local loopback interface.

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. When applying SLAAC to an interface, note that the MAC address of the default VLAN is applied to the interface if the interface does not have its own MAC address.

If SLAAC is not suitable then a network can use stateful configuration with DHCPv6 (Dynamic Host Configuration Protocol version 6) Relay, or hosts can be configured statically. See ip dhcp-relay server-address for the DHCPv6 Relay server command description and examples. See the IP Feature Overview and Configuration Guide for more information about DNS Relay.

Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them. See the ipv6 enable command for more information.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the ipv6 enable command then it will not be removed using a **no ipv6 address** command.

Examples To enable SLAAC on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address autoconfig
```

To disable SLAAC on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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 a VLAN interface or a local loopback interface.

Example To configure the suffix to use when generating an address from prefix information on vlan2, use the command:

```
awplus# configure terminal
awplus(config)# interface vlan2
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 a VLAN interface or a local loopback interface.

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 the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
```

To disable IPv6 with only a link-local IPv6 address on the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 enable
```

Related commands

ipv6 address

ipv6 address autoconfig

ipv6 address dhcp

ipv6 nd prefix

show ipv6 interface

show ipv6 route

show running-config

ipv6 eui64-linklocal

Overview When IPv6 is enabled on an interface, an EUI link-local address is generated and installed on the interface. In other words, **ipv6 eui64-linklocal** is enabled by default on any IPv6 enabled interface.

Use the **no** variant of this command to disallow the automatic generation of the EUI-64 link-local address on an IPv6 enabled interface.

Syntax

```
ipv6 eui64-linklocal
no ipv6 eui64-linklocal
```

Default The command **ipv6 eui64-linklocal** is enabled by default on any IPv6 enabled interface.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Example To enable IPv6 on the interface vlan1, 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 vlan1
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.

NOTE: *Use this command to enable IPv6 unicast routing before configuring either RIPng or OSPFv3 IPv6 routing protocols and static or multicast IPv6 routing.*

Before using PIM-SMv6 commands, IPv6 must be enabled on an interface with the ipv6 enable command, IPv6 forwarding must be enabled globally for routing IPv6 with the ipv6 forwarding command, and IPv6 multicasting must be enabled globally with the ipv6 multicast-routing command.

Syntax

```
ipv6 forwarding
no ipv6 forwarding
```

Mode Global Configuration

Default IPv6 unicast forwarding is disabled by default.

Usage notes Enable IPv6 unicast forwarding globally for all interfaces on your device with this command. Use the **no** variant of this command to disable IPv6 unicast forwarding globally for all interfaces on your device.

IPv6 unicast forwarding allows devices to communicate with devices that are more than one hop away, providing that there is a route to the destination address. If IPv6 forwarding is not enabled then pings to addresses on devices that are more than one hop away will fail, even if there is a route to the destination address.

Examples To enable IPv6 unicast routing, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
```

To disable IPv6 unicast routing, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 forwarding
```

Related commands

ipv6 enable

ipv6 multicast-routing

ipv6 icmp error-interval

Overview Use this command to limit how often IPv6 ICMP error messages are sent. The maximum frequency of messages is specified in milliseconds.

Use the **no** variant of this command to reset the frequency to the default

Syntax

```
ipv6 icmp error-interval <interval>
no ipv6 icmp error-interval
```

Parameter	Description
<interval>	0-2147483647, interval in milliseconds.

Default 1000

Mode Global Configuration

Example To configure the rate to be at most one packet every 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 icmp error-interval 10000
```

To reset the rate to the default of one packet every second, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 icmp error-interval
```

Related commands ip icmp error-interval

ipv6 multicast forward-slow-path-packet

Overview Use this command to enable multicast packets to be forwarded to the CPU. Enabling this command will ensure that the layer L3 MTU is set correctly for each IP multicast group and will apply the value of the smallest MTU among the outgoing interfaces for the multicast group.

It will also ensure that a received packet that is larger than the MTU value will result in the generation of an ICMP Too Big message.

Use the **no** variant of this command to disable the above functionality.

Syntax

```
ipv6 multicast forward-slow-path-packet
no ipv6 multicast forward-slow-path-packet
```

Default Disabled.

Mode Privileged Exec

Example To enable the ipv6 multicast forward-slow-path-packet function, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast forward-slow-path-packet
```

Related commands show ipv6 forwarding

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 a VLAN interface or a local loopback interface.

Example To enable RA-based default routes on vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 enable
awplus(config-if)# no ipv6 nd accept-ra-pinfo
```

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 a VLAN interface or a local loopback interface.

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 vlan1 without installing a SLAAC address on the interface, use the following commands:

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

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 a VLAN interface or a local loopback interface.

Examples To set the advertised current hop limit to 2 between IPv6 Routers on vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd current-hoplimit 2
```

To reset the advertised current hop limit to the default 0 on vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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

Example To add the domain name 'myexample.com' to the search list, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 nd dns search-list myexample.com
```

To delete all domain names added previously, use the commands:

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

Example To configure vlan2 to send RAs and advertise 2001:DB8::2 as a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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 vlan2
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 a VLAN interface or a local loopback interface.

Usage notes Advertisement flags will not be transmitted unless you have applied the ipv6 nd suppress-ra command. This step is included in the example below.

Example To set the managed address configuration flag on vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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 a VLAN interface or a local loopback interface.

Examples To set the minimum RA interval for the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd minimum-ra-interval 60
```

To remove the minimum RA interval for the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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 a VLAN interface or a local loopback interface.

Usage notes Advertisement flags will not be transmitted unless you have applied the ipv6 nd suppress-ra command. This step is included in the example below.

Example To set the IPv6 other-config-flag on the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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 VLAN interface.

Default Valid-lifetime default is 2592000 seconds (30 days). Preferred-lifetime default is 604800 seconds (7 days).

Mode Interface Configuration for a VLAN interface or a local loopback interface.

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 vlan2, and advertise the address prefix of 2001:0db8::/64, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64
```

To configure the device to issue router advertisements on vlan2, 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 vlan2
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
```

To configure the device to issue router advertisements on vlan2 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 vlan2
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
no-autoconfig
```

To reset router advertisements on vlan2, so the address prefix of 2001:0db8::/64 is not advertised from the device, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/64
```

To reset all router advertisements on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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 a VLAN interface or a local loopback interface.

Usage notes Advertisement flags will not be transmitted unless you have applied the **no ipv6 nd suppress-ra** command as shown in the example below.

Example To set the advertisements interval on vlan2 to be 60 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd ra-interval 60
awplus(config-if)# no ipv6 nd suppress-ra
```

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 a VLAN interface or a local loopback interface.

Usage notes This command specifies the lifetime of the current router to be announced in IPv6 Router Advertisements.

Advertisement flags will not be transmitted unless you have applied the **no ipv6 nd suppress-ra** command. This instruction is included in the example shown below.

Examples To set the advertisement lifetime of 8000 seconds on the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd ra-lifetime 8000
awplus(config-if)# no ipv6 nd suppress-ra
```

Related commands ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd raguard

Overview Use this command to apply the Router Advertisements (RA) Guard feature from the Interface Configuration mode for a device port. This blocks all RA messages received on a device port.

For more information about RA Guard, see the IPv6 Feature Overview and Configuration Guide.

Use the **no** parameter with this command to disable RA Guard for a specified device port.

Syntax

```
ipv6 nd raguard
no ipv6 nd raguard
```

Default RA Guard is not disabled by default.

Mode Interface Configuration for a port.

Usage notes Router Advertisements (RAs) are used by Routers to announce themselves on the link. Applying RA Guard to a device port disallows Router Advertisements and redirect messages. RA Guard blocks RAs from untrusted hosts. Blocking RAs stops untrusted hosts from flooding malicious RAs and stops any misconfigured hosts from disrupting traffic on the local network.

Enabling RA Guard on a port blocks RAs from a connected host and indicates the port and host are untrusted. Disabling RA Guard on a port allows RAs from a connected host and indicates the port and host are trusted. Ports and hosts are trusted by default to allow RAs.

Example To enable RA Guard on port1.0.1-port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# ipv6 nd raguard
```

To verify RA Guard is enabled on port1.0.1, use the command:

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

To disable RA Guard on port1.0.1-port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# no ipv6 nd raguard
```

When RA Guard is disabled on a port it is not displayed in **show running-config** output.

Output Example output from using **show running-config interface port1.0.1** to verify RA Guard:

```
!
interface port1.0.1
 switchport mode access

 ipv6 nd raguard
!
```

Related commands show running-config interface

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 a VLAN interface or a local loopback interface.

Usage notes This command specifies the reachable time of the current router to be announced in IPv6 Router Advertisements.

Advertisement flags will not be transmitted unless you have applied 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 the VLAN interface vlan2 to be 1800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd reachable-time 1800000
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the reachable-time in router advertisements on the VLAN interface vlan2 to an unspecified reachable-time (0 milliseconds), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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 a VLAN interface or a local loopback interface.

Examples To set the retransmission-time of Neighbor Solicitation on the VLAN interface vlan2 to be 800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd retransmission-time 800000
```

To reset the retransmission-time of Neighbor Solicitation on the VLAN interface vlan2 to the default 1000 milliseconds (1 second), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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

Example To configure a route of 2001:DB8:1::/48 on VLAN1, with a lifetime of 6000 seconds and a high preference, use the commands:

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

Example To set the router preference to high on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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 a VLAN interface or a local loopback interface.

Example To enable the transmission of router advertisements from vlan2 on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 nd suppress-ra
```

Related commands

ipv6 nd ra-interval

ipv6 nd router-preference

ipv6 nd prefix

ipv6 neighbor

Overview Use this command to add a static IPv6 neighbor entry.

Use the **no** variant of this command to remove a specific IPv6 neighbor entry.

Syntax

```
ipv6 neighbor <ipv6-address> <vlan-name> <mac-address>
<port-list>
```

```
no ipv6 neighbor <ipv6-address> <vlan-name> <port-list>
```

Parameter	Description
<ipv6-address>	Specify the neighbor's IPv6 address in the format X:X::X:X.
<vlan-name>	Specify the neighbor's VLAN name.
<mac-address>	Specify the MAC hardware address in hexadecimal notation in the format HHHH.HHHH.HHHH.
<port-list>	Specify the port number, or port range.

Mode Global Configuration

Usage notes Use this command to clear a specific IPv6 neighbor entry. To clear all dynamic address entries, use the clear ipv6 neighbors command.

Example To create a static neighbor entry for IPv6 address 2001:0db8::a2, on vlan2, with MAC address 0000.cd28.0880, on port1.0.1, use the command:

```
awplus# configure terminal
```

```
awplus(config)# ipv6 neighbor 2001:0db8::a2 vlan2
0000.cd28.0880 port1.0.1
```

Related commands clear ipv6 neighbors

show ipv6 neighbors

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 advertise routes to neighbors and forward packets.

The **no** variant of this command removes the static route.

Syntax

```
ipv6 route <dest-prefix> <dest-prefix/length>
[<src-prefix/length>] {<gateway-ip>|<gateway-name>}
[<distvalue>]
```

```
no ipv6 route <dest-prefix> <dest-prefix/length>
[<src-prefix/length>] {<gateway-ip>|<gateway-name>}
[<distvalue>]
```

Parameter	Description
<dest-prefix/ length>	Specifies the IP destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<src-prefix/length>	Specifies the IP source 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 IP gateway (or next hop) address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<gateway-name>	Specifies the name of the gateway (or next hop) interface.
<distvalue>	Specifies the administrative distance for the route. Valid values are from 1 to 255.

Mode Global Configuration

Usage notes You can use administrative distance to determine which routes take priority over other routes.

Example

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 vlan2 32
```

Validation Commands show running-config

show ipv6 route

Command changes Version 5.5.0-0.3: parameter **src-prefix** 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 24-1: 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
```

optimistic-nd

Overview Use this command to enable the optimistic neighbor discovery feature for both IPv4 and IPv6.

Use the **no** variant of this command to disable the optimistic neighbor discovery feature.

Syntax

```
optimistic-nd
no optimistic-nd
```

Default The optimistic neighbor discovery feature is enabled by default.

Mode Interface Configuration for a VLAN interface.

Usage notes The optimistic neighbor discovery feature allows the device, after learning an IPv4 or IPv6 neighbor, to refresh the neighbor before the neighbor is deleted from the hardware L3 switching table. The device puts the neighbor entry into the ‘stale’ state in the software switching table if is it not refreshed, then the 'stale' neighbors are deleted from the hardware L3 switching table.

The optimistic neighbor discovery feature enables the device to sustain L3 traffic switching to a neighbor without interruption. Without the optimistic neighbor discovery feature enabled L3 traffic is interrupted when a neighbor is ‘stale’ and is then deleted from the L3 switching table.

If a neighbor receiving optimistic neighbor solicitations does not answer optimistic neighbor solicitations with neighbor advertisements, then the neighbor will be put into the ‘stale’ state, and subsequently deleted from both the software and the hardware L3 switching tables.

Examples To enable the optimistic neighbor discovery feature on vlan2, use the following commands:

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

To disable the optimistic neighbor discovery feature on vlan2, use the following commands:

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

Related commands show running-config

ping ipv6

Overview This command sends a query to another IPv6 host (send Echo Request messages).

Syntax

```
ping ipv6 {<host>|<ipv6-address>} [repeat
{<1-2147483647>|continuous}] [size <10-1452>] [interface
<interface-list>] [timeout <1-65535>]
```

Parameter	Description
<ipv6-addr>	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
<hostname>	The destination hostname.
repeat	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
size *<10-1452>*	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
interface *<interface-list>*	The interface or range of configured IP interfaces to use as the source in the IP header of the ping packet. The interface can be one of: • a VLAN (e.g. vlan2) • the loopback interface (lo) • a continuous range of interfaces separated by a hyphen (e.g. vlan10-20) • a comma-separated list (e.g. vlan1,vlan10-20). 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 24-1: Example output from the **show ipv6 forwarding** command

```
awplus#show ipv6 forwarding
ipv6 forwarding is on
```

show ipv6 interface

Overview Use this command to display brief information about interfaces and the IPv6 address assigned to them.

Syntax `show ipv6 interface [brief|<interface-list>] [nd]`

Parameter	Description
`brief`	Specify this optional parameter to display brief IPv6 interface information.
<interface-list>	The interfaces to display information about. An interface-list can be: • a VLAN (e.g. vlan2) • the loopback interface (lo) • a continuous range of interfaces separated by a hyphen (e.g. vlan10-20) • a comma-separated list (e.g. vlan1,vlan10-20). 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 24-2: Example output from the **show ipv6 interface brief** command

```
awplus#show ipv6 interface brief
Interface     IPv6-Address                                Status      Protocol
lo            unassigned                                  admin up    running
vlan1         2001:db8::1/48                              admin up    down
              fe80::215:77ff:fee9:5c50/64
```

Related commands 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 devices IPv6 neighbors, use the following command:

```
awplus# show ipv6 neighbors
```

Output Figure 24-3: Example output of the **show ipv6 neighbors** command

```
IPv6 Address                    MAC Address    Interface          Port      Type
fe80::290:bff:fe3e:44dc         0090.0b3e.44dc vlan1              po3       dynamic
fd32:b1f0:dff7:ab03::1          0090.0b3e.44dc vlan1              po3       dynamic
fe80::2                         eccd.6ddf.6d41 vlan2              po4       static
```

Related commands clear ipv6 neighbors

ipv6 neighbor

show ipv6 route

Overview Use this command to display the IPv6 routing table for a protocol or from a particular table.

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

Syntax

```
show ipv6 route
[bgp|connected|database|ospf|rip|static|summary|<ipv6-address>
|<ipv6-prefix/prefix-length>]
```

Parameter	Description
`bgp`	Displays only the routes learned from BGP.
`connected`	Displays only the routes learned from connected interfaces.
`database`	Displays only the IPv6 routing information extracted from the database.
`ospf`	Displays only the routes learned from OSPFv3.
`rip`	Displays only the routes learned from RIPng.
`static`	Displays only the IPv6 static routes you have configured.
`summary`	Displays summary information from the IPv6 routing table.
`<ipv6-address>`	Displays the routes for the specified address in the IPv6 routing table.
`<ipv6-prefix>/<prefix-length>`	Displays only the routes for the specified IPv6 prefix.

Mode User Exec and Privileged Exec

Example To display all IPv6 routes with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

To display all database entries for all IPv6 routes, use the following command:

```
awplus# show ipv6 route database
```

Output Figure 24-4: 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, vlan10
C   2001:db8::a:0:0:0:0/64 via ::, vlan10
C   2001:db8::14:0:0:0:0/64 via ::, vlan20
C   2001:db8::0:0:0:0/64 via ::, vlan30
C   2001:db8::28:0:0:0:0/64 via ::, vlan40
C   2001:db8::fa:0:0:0:0/64 via ::, vlan250
C   2001:db8::/64 via ::, vlan250
C   2001:db8::/64 via ::, vlan40
C   2001:db8::/64 via ::, vlan20
C   2001:db8::/64 via ::, vlan10
```

Output Figure 24-5: 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 24-6: 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

25 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 971
- "ipv6 route" on page 973
- "max-fib-routes" on page 974
- "max-static-routes" on page 975
- "maximum-paths" on page 976
- "show ip route" on page 977
- "show ip route database" on page 980
- "show ip route summary" on page 982
- "show ipv6 route" on page 983
- "show ipv6 route summary" on page 985

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>]
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. Enter the name of the VLAN or its VID. You can also enter 'null' as an interface. Specify a 'null' interface to add a null or blackhole route to the device. The gateway IP address or the interface is required.
<distance>	The administrative distance for the static route in the range 1 to 255. Static routes by default have an administrative distance of 1, which gives them the highest priority possible.

Mode Global Configuration

Default The default administrative distance for a static route is 1.

Usage notes You can use administrative distance to determine which routes take priority over other routes.

Specify a 'Null' interface to add a null or blackhole route to the switch. A null or blackhole route is a routing table entry that does not forward packets, so any packets sent to it are dropped.

Examples To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at 10.10.0.2 with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To remove the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at 10.10.0.2 with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# no ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To specify a null or blackhole route 192.168.4.0/24, so packets forwarded to this route are dropped, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.4.0/24 null
```

To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at 10.10.0.2 with an administrative distance of 128, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
128
```

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 advertise routes to neighbors and forward packets.

The **no** variant of this command removes the static route.

Syntax

```
ipv6 route <dest-prefix> <dest-prefix/length>
[<src-prefix/length>] {<gateway-ip>|<gateway-name>}
[<distvalue>]
```

```
no ipv6 route <dest-prefix> <dest-prefix/length>
[<src-prefix/length>] {<gateway-ip>|<gateway-name>}
[<distvalue>]
```

Parameter	Description
<dest-prefix/ length>	Specifies the IP destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<src-prefix/length>	Specifies the IP source 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 IP gateway (or next hop) address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<gateway-name>	Specifies the name of the gateway (or next hop) interface.
<distvalue>	Specifies the administrative distance for the route. Valid values are from 1 to 255.

Mode Global Configuration

Usage notes You can use administrative distance to determine which routes take priority over other routes.

Example

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 vlan2 32
```

Validation Commands show running-config

show ipv6 route

Command changes Version 5.5.0-0.3: parameter **src-prefix** added

max-fib-routes

Overview This command enables you to control the maximum number of FIB routes configured. It operates by providing parameters that enable you to configure preset maximums and warning message thresholds.

NOTE: *For static routes use the max-static-routes command.*

Use the **no** variant of this command to set the maximum number of FIB routes to the default of 4294967294 FIB routes.

Syntax

```
max-fib-routes <1-4294967294> [<1-100>|warning-only]
no max-fib-routes
```

Parameter	Description
`max-fib-routes`	This is the maximum number of routes that can be stored in the device's Forwarding Information dataBase. In practice, other practical system limits would prevent this maximum being reached.
<1-4294967294>	The allowable configurable range for setting the maximum number of FIB-routes.
<1-100>	This parameter enables you to optionally apply a percentage value. This percentage will be based on the maximum number of FIB routes you have specified. This will cause a warning message to appear when your routes reach your specified percentage value. Routes can continue to be added until your configured maximum value is reached.
`warning-only`	This parameter enables you to optionally apply a warning message. If you set this option a warning message will appear if your maximum configured value is reached. Routes can continue to be added until your device reaches either the maximum capacity value of 4294967294, or a practical system limit.

Default The default number of FIB routes is the maximum number of FIB routes (4294967294).

Mode Global Configuration

Examples To set the maximum number of dynamic routes to 2000 and warning threshold of 75%, use the following commands:

```
awplus# config terminal
awplus(config)# max-fib-routes 2000 75
```

max-static-routes

Overview Use this command to set the maximum number of static routes, excluding FIB (Forwarding Information Base) routes.

NOTE: *For FIB routes use the max-fib-routes command.*

Use the **no** variant of this command to set the maximum number of static routes to the default of 1000 static routes.

Syntax

```
max-static-routes <1-1000>
no max-static-routes
```

Default The default number of static routes is the maximum number of static routes (1000).

Mode Global Configuration

Example To reset the maximum number of static routes to the default maximum, use the command:

```
awplus# configure terminal
awplus(config)# no max-static-routes
```

NOTE: *Static routes are applied before adding routes to the RIB (Routing Information Base). Therefore, rejected static routes will not appear in the running config.*

Related commands max-fib-routes

maximum-paths

Overview This command enables ECMP on your device, and sets the maximum number of paths that each route has in the Forwarding Information Base (FIB). ECMP is enabled by default.

The **no** variant of this command sets the maximum paths to the default of 4.

Syntax

```
maximum-paths <1-8>
no maximum-paths
```

Parameter	Description
<1-8>	The maximum number of paths that a route can have in the FIB.

Default By default the maximum number of paths is 4.

Mode Global Configuration

Examples To set the maximum number of paths for each route in the FIB to 5, use the command:

```
awplus# configure terminal
awplus(config)# maximum-paths 5
```

To set the maximum paths for a route to the default of 4, use the command:

```
awplus# configure terminal
awplus(config)# no maximum-paths
```

show ip route

Overview Use this command to display routing entries in the FIB (Forwarding Information Base). The FIB contains the best routes to a destination, and your device uses these routes when forwarding traffic. You can display a subset of the entries in the FIB based on protocol.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > output redirection token.

Syntax

```
show ip route [bgp|connected|ospf|rip|static|
<ip-addr>|<ip-addr/prefix-length>]
```

Parameter	Description
`bgp`	Displays only the routes learned from BGP.
`connected`	Displays only the routes learned from connected interfaces.
`ospf`	Displays only the routes learned from OSPF.
`rip`	Displays only the routes learned from RIP.
`static`	Displays only the static routes you have configured.
<ip-addr>	Displays the routes for the specified address. Enter an IPv4 address.
<ip-addr/prefix-length>	Displays the routes for the specified network. Enter an IPv4 address and prefix length.

Mode User Exec and Privileged Exec

Examples To display the static routes in the FIB, use the command:

```
awplus# show ip route static
```

To display the OSPF routes in the FIB, use the command:

```
awplus# show ip route ospf
```

Output Each entry in the output from this command has a code preceding it, indicating the source of the routing entry. For example, O indicates OSPF as the origin of the route. The first few lines of the output list the possible codes that may be seen with the route entries.

Typically, route entries are composed of the following elements:

- code
- a second label indicating the sub-type of the route
- network or host IP address
- administrative distance and metric

- next hop IP address
- outgoing interface name
- time since route entry was added

Figure 25-1: 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

O       10.10.37.0/24 [110/11] via 10.10.31.16, vlan2, 00:20:54
C       3.3.3.0/24 is directly connected, vlan1
C       10.10.31.0/24 is directly connected, vlan2
C       10.70.0.0/24 is directly connected, vlan4
O E2    14.5.1.0/24 [110/20] via 10.10.31.16, vlan2, 00:18:56
C       33.33.33.33/32 is directly connected, lo
```

Connected Route The connected route entry consists of:

```
C       10.10.31.0/24 is directly connected, vlan2
```

This route entry denotes:

- Route entries for network 10.10.31.0/24 are derived from the IP address of local interface vlan2.
- These routes are marked as Connected routes (C) and always preferred over routes for the same network learned from other routing protocols.

OSPF Route The OSPF route entry consists of:

```
O       10.10.37.0/24 [110/11] via 10.10.31.16, vlan2, 00:20:54
```

This route entry denotes:

- This route in the network 10.10.37.0/24 was added by OSPF.
- This route has an administrative distance of 110 and metric/cost of 11.
- This route is reachable via next hop 10.10.31.16.
- The outgoing local interface for this route is vlan2.
- This route was added 20 minutes and 54 seconds ago.

OSPF External Route The OSPF external route entry consists of:

```
O E2    14.5.1.0/24 [110/20] via 10.10.31.16, vlan2, 00:18:56
```

This route entry denotes that this route is the same as the other OSPF route explained above; the main difference is that it is a Type 2 External OSPF route.

Related commands

ip route

maximum-paths

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 [bgp|connected|ospf|rip|static]
```

Parameter	Description
`bgp`	Displays only the routes learned from BGP.
`connected`	Displays only the routes learned from connected interfaces.
`ospf`	Displays only the routes learned from OSPF.
`rip`	Displays only the routes learned from RIP.
`static`	Displays only the static routes you have configured.

Mode User Exec and Privileged Exec

Example To display the static routes in the RIB, use the command:

```
awplus# show ip route database static
```

Output Figure 25-2: 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

O    *> 9.9.9.9/32 [110/31] via 10.10.31.16, vlan2, 00:19:21
O       10.10.31.0/24 [110/1] is directly connected, vlan2, 00:28:20
C    *> 10.10.31.0/24 is directly connected, vlan2
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, vlan2
O       10.10.34.0/24 [110/31] via 10.10.31.16, vlan2, 00:21:19
O    *> 10.10.37.0/24 [110/11] via 10.10.31.16, vlan2, 00:21:19
C    *> 10.30.0.0/24 is directly connected, vlan6
S    *> 11.22.11.0/24 [1/0] via 10.10.31.16, vlan2
O E2 *> 14.5.1.0/24 [110/20] via 10.10.31.16,vlan2, 00:19:21
O       16.16.16.16/32 [110/11] via 10.10.31.16, vlan2, 00:21:19
S    *> 16.16.16.16/32 [1/0] via 10.10.31.16, vlan2
O    *> 17.17.17.17/32 [110/31] via 10.10.31.16, vlan2, 00:21:19
C    *> 45.45.45.45/32 is directly connected, lo
O    *> 55.55.55.55/32 [110/21] via 10.10.31.16, vlan2, 00:21:19
C    *> 127.0.0.0/8 is directly connected, lo
```

Related commands maximum-paths

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 25-3: 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
ospf            2
Total           8
```

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
[bgp|connected|database|ospf|rip|static|summary|<ipv6-address>
|<ipv6-prefix/prefix-length>]
```

Parameter	Description
`bgp`	Displays only the routes learned from BGP.
`connected`	Displays only the routes learned from connected interfaces.
`database`	Displays only the IPv6 routing information extracted from the database.
`ospf`	Displays only the routes learned from OSPFv3.
`rip`	Displays only the routes learned from RIPng.
`static`	Displays only the IPv6 static routes you have configured.
`summary`	Displays summary information from the IPv6 routing table.
`<ipv6-address>`	Displays the routes for the specified address in the IPv6 routing table.
`<ipv6-prefix>/<prefix-length>`	Displays only the routes for the specified IPv6 prefix.

Mode User Exec and Privileged Exec

Example To display all IPv6 routes with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

To display all database entries for all IPv6 routes, use the following command:

```
awplus# show ipv6 route database
```

Output Figure 25-4: 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, vlan10
C   2001:db8::a:0:0:0:0/64 via ::, vlan10
C   2001:db8::14:0:0:0:0/64 via ::, vlan20
C   2001:db8::0:0:0:0/64 via ::, vlan30
C   2001:db8::28:0:0:0:0/64 via ::, vlan40
C   2001:db8::fa:0:0:0:0/64 via ::, vlan250
C   2001:db8::/64 via ::, vlan250
C   2001:db8::/64 via ::, vlan40
C   2001:db8::/64 via ::, vlan20
C   2001:db8::/64 via ::, vlan10
```

Output Figure 25-5: 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 25-6: 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

26 RIP Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure RIP.

For information about configuring RIP, see the RIP Feature Overview and Configuration Guide.

Command List

- "accept-lifetime" on page 988
- "alliedware-behavior" on page 990
- "cisco-metric-behavior (RIP)" on page 992
- "clear ip rip route" on page 993
- "debug rip" on page 994
- "default-information originate (RIP)" on page 995
- "default-metric (RIP)" on page 996
- "distance (RIP)" on page 997
- "distribute-list (RIP)" on page 998
- "fullupdate (RIP)" on page 999
- "ip summary-address rip" on page 1000
- "ip prefix-list" on page 1001
- "ip rip authentication key-chain" on page 1003
- "ip rip authentication mode" on page 1005
- "ip rip authentication string" on page 1008
- "ip rip receive-packet" on page 1010
- "ip rip receive version" on page 1011
- "ip rip send-packet" on page 1012

- "ip rip send version" on page 1013
- "ip rip send version 1-compatible" on page 1015
- "ip rip split-horizon" on page 1017
- "key" on page 1018
- "key chain" on page 1019
- "key-string" on page 1020
- "maximum-prefix" on page 1021
- "neighbor (RIP)" on page 1022
- "network (RIP)" on page 1023
- "offset-list (RIP)" on page 1024
- "passive-interface (RIP)" on page 1025
- "recv-buffer-size (RIP)" on page 1026
- "redistribute (RIP)" on page 1027
- "restart rip graceful" on page 1028
- "rip restart grace-period" on page 1029
- "route (RIP)" on page 1030
- "router rip" on page 1031
- "send-lifetime" on page 1032
- "show debugging rip" on page 1034
- "show ip prefix-list" on page 1035
- "show ip protocols rip" on page 1036
- "show ip rip" on page 1037
- "show ip rip database" on page 1038
- "show ip rip interface" on page 1039
- "timers (RIP)" on page 1040
- "undebug rip" on page 1041
- "version (RIP)" on page 1042

accept-lifetime

Overview Use this command to specify the time period during which the authentication key on a key chain is received as valid.

Use the **no** variant of this command to remove a specified time period for an authentication key on a key chain as set previously with the **accept-lifetime** command.

Syntax

```
accept-lifetime <start-date> {<end-date>|
duration <seconds>|infinite}
```

```
no accept-lifetime
```

Parameter	Description	
<start-date>	Specifies the start time and date in the format: *<hh:mm:ss> <day> <month> <year>* or *<hh:mm:ss> <month> <day> <year>*, where:	
	<hh:mm:ss>	The time of the day, in hours, minutes and seconds
	<day>	<1-31> The day of the month
	<month>	The month of the year (the first three letters of the month, for example, Jan)
	<year>	<1993-2035> The year
<end-date>	Specifies the end time and date in the format: *<hh:mm:ss> <day> <month> <year>* or *<hh:mm:ss> <month> <day> <year>*, where:	
	<hh:mm:ss>	The time of the day, in hours, minutes and seconds
	<day>	<1-31> The day of the month
	<month>	The month of the year (the first three letters of the month, for example, Jan)
	<year>	<1993-2035> The year
<seconds>	<1-2147483646> Duration of the key in seconds.	
infinite	Never expires.	

Mode Keychain-key Configuration

Examples The following examples show the setting of accept-lifetime for key 1 on the key chain named “mychain”.

```
awplus# configure terminal
```

```
awplus(config)# key chain mychain
```

```
awplus(config-keychain)# key 1
```

```
awplus(config-keychain-key)# accept-lifetime 03:03:01 Sep 3
2016 04:04:02 Oct 6 2016
```

or:

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# accept-lifetime 03:03:01 3 Sep
2016 04:04:02 6 Oct 2016
```

Related commands

key

key-string

key chain

send-lifetime

alliedware-behavior

Overview This command configures your device to exhibit AlliedWare behavior when sending RIPv1 response/update messages. Configuring for this behavior may be necessary if you are replacing an AlliedWare device with an AlliedWare Plus device and wish to ensure consistent RIPv1 behavior.

Use the **no** variant of this command to implement AlliedWare Plus behavior.

This command has no impact on devices running RIPv2. Reception and transmission can be independently altered to conform to AlliedWare standard.

Syntax

```
alliedware-behavior {rip1-send|rip1-recv}
no alliedware-behavior {rip1-send|rip1-recv}
```

Parameter	Description
`rip1-send`	Configures the router to behave in AlliedWare mode when **sending** update messages.
`rip1-recv`	Configures the router to behave in AlliedWare mode when **receiving** update messages.

Default By default when sending out RIPv1 updates on an interface, if the prefix (learned through RIPv2 or otherwise redistributed into RIP) being advertised does not match the subnetting used on the outgoing RIPv1 interface it will be filtered. The **alliedware-behavior** command returns your router's RIPv1 behavior to the AlliedWare format, where the prefix will be advertised as-is.

For example, if a RIPv1 update is being sent over interface 192.168.1.4/26, by default the prefix 192.168.1.64/26 will be advertised, but the prefix 192.168.1.144/28 will be filtered because the mask /28 does not match the interface's mask of /26. If **alliedware-behavior rip1-send** is configured, 192.168.1.144 would be sent as-is.

Mode Router Configuration

Examples To configure your device for **AlliedWare**-like behavior when sending and receiving RIPv1 update messages, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# alliedware-behavior rip1-send
awplus(config-router)# alliedware-behavior rip1-recv
```

To return your device to **AlliedWare Plus**-like behavior when sending and receiving RIPv1 update messages, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no alliedware-behavior rip1-send
awplus(config-router)# no alliedware-behavior rip1-recv
```

Validation Commands

show ip protocols rip

show running-config

Related commands

fullupdate (RIP)

cisco-metric-behavior (RIP)

Overview Use this command to enable or disable the RIP routing metric update to conform to Cisco's implementation. This command is provided to allow inter-operation with older Cisco devices that do not conform to the RFC standard for RIP route metrics.

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

Syntax

```
cisco-metric-behavior {enable|disable}
no cisco-metric-behavior
```

Parameter	Description
`enable`	Enables updating the metric consistent with Cisco.
`disable`	Disables updating the metric consistent with Cisco.

Default By default, the Cisco metric-behavior is disabled.

Mode Router Configuration

Examples To enable the routing metric update to behave as per the Cisco implementation, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# cisco-metric-behavior enable
```

To disable the routing metric update to behave as per the default setting, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no cisco-metric-behavior
```

Validation Commands show running-config

clear ip rip route

Overview Use this command to clear specific data from the RIP routing table.

Syntax

```
clear ip rip route <ip-dest-network/prefix-length>
clear ip rip route
{static|connected|rip|ospf|bgp|invalid-routes|all}
```

Parameter	Description
<ip-dest-network/prefix-length>	Removes entries which exactly match this destination address from RIP routing table. Enter the IP address and prefix length of the destination network.
`static`	Removes static entries from the RIP routing table.
`connected`	Removes entries for connected routes from the RIP routing table.
`rip`	Removes only RIP routes from the RIP routing table.
`ospf`	Removes only OSPF routes from the RIP routing table.
`bgp`	Removes only BGP routes from the RIP routing table.
`invalid-routes`	Removes routes with metric 16 immediately. Otherwise, these routes are not removed until RIP times out the route after 2 minutes.
`all`	Clears the entire RIP routing table.

Mode Privileged Exec

Usage notes Using this command with the **all** parameter clears the RIP table of all the routes.

Examples To clear the route 10.0.0.0/8 from the RIP routing table, use the following command:

```
awplus# clear ip rip route 10.0.0.0/8
```

debug rip

Overview Use this command to specify the options for the displayed debugging information for RIP events and RIP packets.

Use the **no** variant of this command to disable the specified debug option.

Syntax

```
debug rip {events|nsm|<packet>|all}
no debug rip {events|nsm|<packet>|all}
```

Parameter	Description
`events`	RIP events debug information is displayed.
`nsm`	RIP and NSM communication is displayed.
`<packet>`	`packet [recv|send] [detail]` Specifies RIP packets only.
`recv`	Specifies that information for received packets be displayed.
`send`	Specifies that information for sent packets be displayed.
`detail`	Displays detailed information for the sent or received packet.
`all`	Displays all RIP debug information.

Default Disabled

Mode Privileged Exec and Global Configuration

Example The following example displays information about the RIP packets that are received and sent out from the device.

```
awplus# debug rip packet
```

Related commands undebug rip

default-information originate (RIP)

Overview Use this command to generate a default route into the Routing Information Protocol (RIP).

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

Syntax
```
default-information originate
no default-information originate
```

Default Disabled

Mode Router Configuration

Usage If routes are being redistributed into RIP and the router's route table contains a default route, within one of the route categories that are being redistributed, the RIP protocol will advertise this default route, irrespective of whether the **default-information originate** command has been configured or not. However, if the router has not redistributed any default route into RIP, but you want RIP to advertise a default route anyway, then use this command.

This will cause RIP to create a default route entry in the RIP database. The entry will be of type RS (Rip Static). Unless actively filtered out, this default route will be advertised out every interface that is sending RIP. Split horizon does not apply to this route, as it is internally generated. This operates quite similarly to the OSPF **default-information originate always** command.

Example
```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# default-information originate
```

default-metric (RIP)

Overview Use this command to specify the metrics to be assigned to redistributed RIP routes.

Use the **no** variant of this command to reset the RIP metric back to its default (1).

Syntax

```
default-metric <metric>
no default-metric [<metric>]
```

Parameter	Description
<metric>	<1-16> Specifies the value of the default metric.

Default By default, the RIP metric value is set to 1.

Mode RIP Router Configuration

Usage notes This command is used with the redistribute (RIP) command to make the routing protocol use the specified metric value for all redistributed routes, regardless of the original protocol that the route has been redistributed from.

Examples This example assigns the cost of 10 to the routes that are redistributed into RIP.

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# default-metric 10
awplus(config-router)# redistribute ospf
awplus(config-router)# redistribute connected
```

Related commands redistribute (RIP)

distance (RIP)

Overview This command sets the administrative distance for RIP routes. Your device uses this value to select between two or more routes to the same destination obtained from two different routing protocols. The route with the smallest administrative distance value is added to the Forwarding Information Base (FIB). For more information, see the Route Selection Feature Overview and Configuration Guide.

The **no** variant of this command sets the administrative distance for the RIP route to the default of 120.

Syntax

```
distance <1-255> [<ip-addr/prefix-length> [<access-list>]]
no distance [<1-255>] [<ip-addr/prefix-length> [<access-list>]]
```

Parameter	Description
<1-255>	The administrative distance value you are setting for this RIP route.
<ip-addr/prefix-length>	The network IP address and prefix-length that you are changing the administrative distance for.
<access-list>	Specifies the access-list name. This access list specifies which routes within the specified network this command applies to.

Mode RIP Router Configuration

Examples To set the administrative distance to 8 for the RIP routes within the 10.0.0.0/8 network that match the access-list "mylist", use the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# distance 8 10.0.0.0/8 mylist
```

To set the administrative distance to the default of 120 for the RIP routes within the 10.0.0.0/8 network that match the access-list "mylist", use the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no distance 8 10.0.0.0/8 mylist
```

distribute-list (RIP)

Overview Use this command to filter incoming or outgoing route updates using the access-list or the prefix-list.

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

Syntax

```
distribute-list {<access-list> | prefix <prefix-list>} {in|out}
[<interface>]
```

```
no distribute-list {<access-list> | prefix <prefix-list>}
{in|out}  [<interface>]
```

Parameter	Description
`prefix`	Filter prefixes in routing updates.
<access-list>	Specifies the IPv4 access-list number or name to use.
<prefix-list>	Specifies the name of the IPv4 prefix-list to use.
`in`	Filter incoming routing updates.
`out`	Filter outgoing routing updates.
<interface>	The interface on which distribute-list applies. For instance: `vlan2`

Default Disabled

Mode RIP Router Configuration

Usage notes Filter out incoming or outgoing route updates using access-list or prefix-list. If you do not specify the name of the interface, the filter will be applied to all interfaces.

Examples In this example the following commands are used to apply an access list called myfilter to filter incoming routing updates in `vlan2`

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# distribute-list prefix myfilter in vlan2
```

Related commands access-list extended (named)

ip prefix-list

fullupdate (RIP)

Overview Use this command to specify which routes RIP should advertise when performing a triggered update. By default, when a triggered update is sent, RIP will only advertise those routes that have changed since the last update. When **fullupdate** is configured, the device advertises the full RIP route table in outgoing triggered updates, including routes that have not changed. This enables faster convergence times, or allows inter-operation with legacy network equipment, but at the expense of larger update messages.

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

Syntax

```
fullupdate
no fullupdate
```

Default By default this feature is disabled.

Mode RIP Router Configuration

Example To enable the fullupdate (RIP) function, use the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# fullupdate
```

ip summary-address rip

Overview Use this command to configure a summary IP address on a RIPv2 interface.

Use the **no** variant of this command to remove a summary IP address from a selected RIPv2 interface.

Syntax

```
ip summary-address rip {<ip-address/prefix-length>}
no ip summary-address rip {<ip-address/prefix-length>}
```

Parameter	Description
<ip-address/prefix-length>	The summary IPv4 address to be advertised

Usage notes Route summarization is a technique that helps network administrators in reducing the size of the routing tables by advertising a single super-network that covers a range of subnets.

You statically configure an IP summary address on a router interface. The router then advertises the summary address downstream through this interface. This means that:

- all the routers that are downstream from the configured interface will receive only the summary route, and none of the child routes via the RIP advertisement.
- As long as any of the child routes is valid, the router will propagate the summary route. But when the last child that is part of the summarized range disappears, then the router will stop advertising the summary route through the interface.

This command will be rejected if there is no IP address configured on the interface.

NOTE: *Manual route summarization is not supported when the interface/router is running in RIPv1.*

Example The subnets: 10.4.1.0/24, 10.4.2.128/25, 10.4.3.0/24 can be summarized and advertised as 10.4.0.0/16 on vlan1 using the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip summary-address rip 10.4.0.0/16
```

Related commands show ip rip database

show ip protocols rip

Command changes Version 5.4.8-0.2 command added

ip prefix-list

Overview Use this command to create an entry for an IPv4 prefix list.

Use the **no** variant of this command to delete the IPv4 prefix-list entry.

Syntax

```
ip prefix-list <list-name> [seq <1-429496725>] {deny|permit}
{any|<ip-prefix>} [ge <0-32>] [le <0-32>]
ip prefix-list <list-name> description <text>
ip prefix-list sequence-number
no ip prefix-list <list-name> [seq <1-429496725>]
no ip prefix-list <list-name> [description <text>]
no ip prefix-list sequence-number
```

Parameter	Description
<list-name>	Specifies the name of a prefix list.
seq *<1-429496725>*	Sequence number of the prefix list entry.
deny	Specifies that the prefixes are excluded from the list.
permit	Specifies that the prefixes are included in the list.
<ip-prefix>	Specifies the IPv4 address and length of the network mask in dotted decimal in the format A.B.C.D/M.
any	Any prefix match. Same as **0.0.0.0/0 le 32**.
ge*<0-32>*	Specifies the minimum prefix length to be matched.
le*<0-32>*	Specifies the maximum prefix length to be matched.
<text>	Text description of the prefix list.
sequence-number	Specify sequence numbers included or excluded in prefix list.

Mode Global Configuration

Usage notes When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the **seq** parameter and place common permits or denials towards the top of the list. If you do not use the **seq** parameter, the sequence values are generated in a sequence of 5.

The parameters **ge** and **le** specify the range of the prefix lengths to be matched. When setting these parameters, set the **le** value to be less than 32, and the **ge** value to be less than or equal to the **le** value and greater than the ip-prefix mask length.

Prefix lists implicitly exclude prefixes that are not explicitly permitted in the prefix list. This means if a prefix that is being checked against the prefix list reaches the end of the prefix list without matching a permit or deny, this prefix will be denied.

Example In the following sample configuration, the last **ip prefix-list** command in the below list matches all, and the first **ip prefix-list** command denies the IP network 76.2.2.0:

```
awplus(config)# router bgp 100
awplus(config-router)# network 172.1.1.0
awplus(config-router)# network 172.1.2.0
awplus(config-router)# neighbor 10.6.5.3 remote-as 300
awplus(config-router)# neighbor 10.6.5.3 prefix-list mylist out
awplus(config-router)# exit
awplus(config)# ip prefix-list mylist seq 5 deny 76.2.2.0/24
awplus(config)# ip prefix-list mylist seq 100 permit any
```

To deny the IP addresses between 10.0.0.0/14 (10.0.0.0 255.252.0.0) and 10.0.0.0/22 (10.0.0.0 255.255.252.0) within the 10.0.0.0/8 (10.0.0.0 255.0.0.0) addressing range, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip prefix-list mylist seq 12345 deny 10.0.0.0/8
ge 14 le 22
```

Related commands

match ip address

neighbor prefix-list

area filter-list

clear ip prefix-list

match route-type

show ip prefix-list

ip rip authentication key-chain

Overview Use this command to enable RIPv2 authentication on an interface and specify the name of the key chain to be used.

Use the **no** variant of this command to disable this function.

Syntax

```
ip rip authentication key-chain <key-chain-name>
no ip rip authentication key-chain
```

Parameter	Description
<key-chain-name>	Specify the name of the key chain. This is an alpha-numeric string, but it cannot include spaces.

Mode Interface Configuration for a VLAN interface.

Usage notes This command can only be used on VLAN interfaces.

Use this command to perform authentication on the interface. Not configuring the key chain results in no authentication at all.

The AlliedWare Plus™ implementation provides the choice of configuring authentication for single key or multiple keys at different times. Use the ip rip authentication string command for single key authentication. Use the ip rip authentication key-chain command for multiple keys authentication. See the RIP Feature Overview and Configuration Guide for illustrated RIP configuration examples.

For multiple key authentication, use the following steps to configure a route to enable RIPv2 authentication using multiple keys at different times:

1) Define a key chain with a key chain name, using the following commands:

```
awplus# configure terminal
awplus(config)# key chain <key-chain-name>
```

2) Define a key on this key chain, using the following command:

```
awplus(config-keychain)# key <keyid>
```

3) Define the password used by the key, using the following command:

```
awplus(config-keychain-key)# key-string <key-password>
```

4) Enable authentication on the desired interface and specify the key chain to be used, using the following commands:

```
awplus# configure terminal
awplus(config)# interface <id>
awplus(config-if)# ip rip authentication key-chain
<key-chain-name>
```

5) Specify the mode of authentication for the given interface (text or MD5), using the following command:

```
awplus(config-if)# ip rip authentication mode {md5|text}
```

Example In the following example of a configuration for multiple keys authentication, a password “toyota” is set for key 1 in key chain “cars”. Authentication is enabled on vlan2 and the authentication mode is set to MD5:

```
awplus# configure terminal
awplus(config)# key chain cars
awplus(config-keychain)# key 1
awplus(config-keychain-key)# key-string toyota
awplus(config-keychain-key)# accept-lifetime 10:00:00 Oct 08 2016 duration 43200
awplus(config-keychain-key)# send-lifetime 10:00:00 Oct 08 2016 duration 43200
awplus(config-keychain-key)# exit
awplus(config-keychain)# exit
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication key-chain cars
awplus(config-if)# ip rip authentication mode md5
```

Example In the following example, the VLAN interface vlan23 is configured to use key-chain authentication with the keychain “mykey”. See the key command for a description of how a key chain is created.

```
awplus# configure terminal
awplus(config)# interface vlan23
awplus(config-if)# ip rip authentication key-chain mykey
```

Related commands

accept-lifetime

send-lifetime

ip rip authentication mode

ip rip authentication string

key

key chain

ip rip authentication mode

Overview Use this command to specify the type of authentication mode used for RIP v2 packets.

Use the **no** variant of this command to restore clear text authentication.

Syntax

```
ip rip authentication mode {md5|text}
no ip rip authentication mode
```

Parameter	Description
`md5`	Uses the keyed MD5 authentication algorithm.
`text`	Specifies clear text or simple password authentication.

Default Text authentication is enabled

Mode Interface Configuration for a VLAN interface.

Usage notes This command can only be used on VLAN interfaces.

The AlliedWare Plus™ implementation provides the choice of configuring authentication for single key or multiple keys at different times. Use the ip rip authentication string command for single key authentication. Use the ip rip authentication key-chain command for multiple keys authentication. See the RIP Feature Overview and Configuration Guide for illustrated RIP configuration examples.

Usage: single key Use the following steps to configure a route to enable RIPv2 authentication using a single key or password:

1) Define the authentication string or password used by the key for the desired interface, using the following commands:

```
awplus# configure terminal
awplus(config)# interface <id>
awplus(config-if)# ip rip authentication string <auth-string>
```

2) Specify the mode of authentication for the given interface (text or MD5), using the following commands:

```
awplus# configure terminal
awplus(config)# interface <id>
awplus(config-if)# ip rip authentication mode {md5|text}
```

Usage: multiple key

For multiple keys authentication, use the following steps to configure a route to enable RIPv2 authentication using multiple keys at different times:

1) Define a key chain with a key chain name, using the following commands:

```
awplus# configure terminal
awplus(config)# key chain <key-chain-name>
```

2) Define a key on this key chain using the following command:

```
awplus(config-keychain)# key <keyid>
```

3) Define the password used by the key, using the following command:

```
awplus(config-keychain-key)# key-string <key-password>
```

4) Enable authentication on the desired interface and specify the key chain to be used, using the following commands:

```
awplus(config-if)# ip rip authentication key-chain
<key-chain-name>
```

5) Specify the mode of authentication for the given interface (text or MD5), using the following commands:

```
awplus(config-if)# ip rip authentication mode {md5|text}
```

Example 1

In the following example of a configuration for multiple keys authentication, a password of "toyota" is set for key 1 in key chain "cars". Authentication is enabled on vlan2 and the authentication mode is set to MD5:

```
awplus# configure terminal
awplus(config)# key chain cars
awplus(config-keychain)# key 1
awplus(config-keychain-key)# key-string toyota
awplus(config-keychain-key)# accept-lifetime 10:00:00 Oct 08
2016 duration 43200
awplus(config-keychain-key)# send-lifetime 10:00:00 Oct 08 2016
duration 43200
awplus(config-keychain-key)# exit
awplus(config-keychain)# exit
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication key-chain cars
awplus(config-if)# ip rip authentication mode md5
```

Example 2

The following example shows MD5 authentication configured on VLAN interface vlan2, ensuring authentication of RIP packets received on this interface.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication mode md5
```

Example 3 The following example specifies “mykey” as the authentication string with MD5 authentication, for the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication string mykey
awplus(config-if)# ip rip authentication mode md5
```

Related commands ip rip authentication string

ip rip authentication key-chain

ip rip authentication string

Overview Use this command to specify the authentication string or password used by a key.

Use the **no** variant of this command to remove the authentication string.

Syntax

```
ip rip authentication string <auth-string>
no ip rip authentication string
```

Parameter	Description
<auth-string>	The authentication string or password used by a key. It is an alpha-numeric string and can include spaces.

Mode Interface Configuration for a VLAN interface.

Usage notes This command can only be used on VLAN interfaces.

The AlliedWare Plus™ implementation provides the choice of configuring authentication for single key or multiple keys at different times. Use this command to specify the password for a single key on an interface. Use the ip rip authentication key-chain command for multiple keys authentication. For information about configuring RIP, see the RIP Feature Overview and Configuration Guide.

Use the following steps to configure a route to enable RIPv2 authentication using a single key or password:

1) Define the authentication string or password used by the key for the desired interface, using the following commands:

```
awplus# configure terminal
awplus(config)# interface <id>
```

2) Specify the mode of authentication for the given interface (text or MD5), using the following commands:

```
awplus# configure terminal
awplus(config-if)# ip rip authentication string <auth-string>
awplus(config)# interface <id>
awplus(config-if)# ip rip authentication mode {md5|text}
```

Example See the example below to specify `mykey` as the authentication string with MD5 authentication for the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication string mykey
awplus(config-if)# ip rip authentication mode md5
```

Example In the following example, the VLAN interface `vlan2` is configured to have an authentication string as `guest`. Any received RIP packet in that interface should have the same string as password.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip authentication string guest
```

Related commands

ip rip authentication key-chain

ip rip authentication mode

ip rip receive-packet

Overview Use this command to configure the interface to enable the reception of RIP packets.

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

Syntax

```
ip rip receive-packet
no ip rip receive-packet
```

Default Receive-packet is enabled

Mode Interface Configuration for a VLAN interface.

Usage This command can only be configured on VLAN interfaces.

Example This example shows packet receiving being turned on for the VLAN interface `vlan3`:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip rip receive-packet
```

Related commands ip rip send-packet

ip rip receive version

Overview Use this command to specify the version of RIP packets accepted on an interface and override the setting of the version command.

Use the **no** variant of this command to use the setting specified by the version (RIP) command.

Syntax

```
ip rip receive version {[1][2]}
no ip rip receive version
```

Parameter	Description
1	Specifies acceptance of RIP version 1 packets on the interface.
2	Specifies acceptance of RIP version 2 packets on the interface.

Default Version 2

Mode Interface Configuration for a VLAN interface.

Usage notes This command can only be used on VLAN interfaces.

This command applies to a specific VLAN interface and overrides any the version specified by the version (RIP) command.

RIP can be run in version 1 or version 2 mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces.

Example In the following example, the VLAN interface `vlan3` is configured to receive both RIP version 1 and 2 packets:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip rip receive version 1 2
```

Related commands version (RIP)

ip rip send-packet

Overview Use this command to enable sending RIP packets through the current interface.

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

Syntax

```
ip rip send-packet
no ip rip send-packet
```

Default Send packet is enabled

Mode Interface Configuration for a VLAN interface.

Usage This command can only be configured on VLAN interfaces.

Example This example shows packet sending being turned on for the VLAN interface `vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip rip send-packet
```

Related commands ip rip receive-packet

ip rip send version

Overview Use this command in Interface Configuration mode to specify the version of RIP packets sent on an interface and override the setting of the version (RIP) command. This mechanism causes RIP version 2 interfaces to send multicast packets instead of broadcasting packets.

Use the **no** variant of this command to use the setting specified by the version (RIP) command.

Syntax

```
ip rip send version {1|2|1 2|2 1}
no ip rip send version
```

Parameter	Description
1	Specifies the sending of RIP version 1 packets out of an interface.
2	Specifies the sending of RIP version 2 packets out of an interface.
12	Specifies the sending of both RIP version 1 and RIP version 2 packets out of an interface.
21	Specifies the sending of both RIP version 2 and RIP version 1 packets out of an interface.

Default RIP version 2 is enabled by default.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to a specific interface and overrides the version specified by the version (RIP) command.

RIP can be run in version 1 or version 2 mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces. Selecting version parameters 1 2 or 2 1 sends RIP version 1 and 2 packets.

Use the ip rip send version 1-compatible command in an environment where you cannot send multicast packets. For example, in environments where multicast is not enabled and where hosts do not listen to multicast.

Examples In the following example, the VLAN interface `vlan4` is configured to send both RIP version 1 and 2 packets.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip rip send version 1 2
```

In the following example, the VLAN interface `vlan4` is configured to send both RIP version 2 and 1 packets.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip rip send version 2 1
```

In the following example, the VLAN interface `vlan4` is configured to send RIP version 1 packets only.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip rip send version 1
```

In the following example, the VLAN interface `vlan4` is configured to send RIP version 2 packets only.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ip rip send version 2
```

In the following example, the VLAN interface `vlan3` is configured to use the RIP version specified by the version (RIP) command.

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# no ip rip send version
```

Related commands

ip rip send version 1-compatible

version (RIP)

ip rip send version 1-compatible

Overview Use this command in Interface Configuration mode to send RIP version 1 compatible packets from a RIP version 2 interfaces to other RIP Interfaces. This mechanism causes RIP version 2 interfaces to send broadcast packets instead of multicasting packets, and is used in environments where multicast is not enabled or where hosts do not listen to multicast.

Use the **no** variant of this command to use the setting specified by the version (RIP) command, and disable the broadcast of RIP version 2 packets that are sent as broadcast packets.

Syntax

```
ip rip send version 1-compatible
no ip rip send version
```

Parameter	Description
`1-compatible`	Specify this parameter to send RIP version 1 compatible packets from a version 2 RIP interface to other RIP interfaces. This mechanism causes version 2 RIP interfaces to broadcast packets instead of multicasting packets.

Default RIP version 2 is enabled by default.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to a specific interface and overrides the version specified by the version (RIP) command.

RIP can be run in version 1 compatible mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces.

Use the ip rip send version command in an environment where you can send multicast packets. For example, in environments where multicast is enabled and where hosts listen to multicast.

Examples In the following example, the VLAN interface `vlan2` is configured to send RIP version 1- compatible packets.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip send version 1-compatible
```

In the following example, the VLAN interface `vlan3` is configured to use the RIP version specified by the version (RIP) command.

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# no ip rip send version
```

Related commands

ip rip send version

version (RIP)

ip rip split-horizon

Overview Use this command to turn on the split-horizon mechanism on the interface.

Use the **no** variant of this command to disable this mechanism.

Syntax

```
ip rip split-horizon [poisoned]
no ip rip split-horizon
```

Parameter	Description
`poisoned`	Performs split-horizon with poison-reverse. See "Usage" below for more information.

Default Split horizon poisoned

Mode Interface Configuration for a VLAN interface.

Usage notes Use this command to avoid including routes in updates sent to the same gateway from which they were learned. Without the **poisoned** parameter, using this command causes routes learned from a neighbor to be omitted from updates sent to that neighbor. With the **poisoned** parameter, using this command causes such routes to be included in updates, but sets their metrics to infinity. This advertises that these routes are not reachable.

Example To turn on split horizon poisoned on vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip rip split-horizon poisoned
```

key

Overview Use this command to manage, add and delete authentication keys in a key-chain.

Use the **no** variant of this command to delete the authentication key.

Syntax

```
key <keyid>
no key <keyid>
```

Parameter	Description
<keyid>	<0-2147483647> Key identifier number.

Mode Keychain Configuration

Usage This command allows you to enter the keychain-key mode where a password can be set for the key.

Example The following example configures a key number 1 and shows the change into a **keychain- key** command mode prompt.

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)#
```

Related commands

key chain

key-string

accept-lifetime

send-lifetime

key chain

Overview Use this command to enter the key chain management mode and to configure a key chain with a key chain name.

Use the **no** variant of this command to remove the key chain and all configured keys.

Syntax

```
key chain <key-chain-name>
no key chain <key-chain-name>
```

Parameter	Description
<key-chain-name>	Specify the name of the key chain to manage.

Mode Global Configuration

Usage This command allows you to enter the keychain mode from which you can specify keys on this key chain.

Example The following example shows the creation of a key chain named `mychain` and the change into **keychain** mode prompt.

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)#
```

Related commands

key

key-string

accept-lifetime

send-lifetime

key-string

Overview Use this command to define the password to be used by a key.

Use the **no** variant of this command to remove a password.

Syntax

```
key-string <key-password>
no key-string
```

Parameter	Description
<key-password>	A string of characters to be used as a password by the key.

Mode Keychain-key Configuration

Usage Use this command to specify passwords for different keys.

Examples In the following example, the password for `key1` in the key chain named `mychain` is set to password **prime**:

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# key-string prime
```

In the following example, the password for `key1` in the key chain named `mychain` is removed:

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# no key-string
```

Related commands

key

key chain

accept-lifetime

send-lifetime

maximum-prefix

Overview Use this command to configure the maximum number of RIP routes stored in the routing table.

Use the **no** variant of this command to disable all limiting of the number of RIP routes stored in the routing table.

Syntax

```
maximum-prefix <maxprefix> [<threshold>]
no maximum-prefix
```

Parameter	Description
<maxprefix>	<1-65535> The maximum number of RIP routes allowed.
<threshold>	<1-100> Percentage of maximum routes to generate a warning. The default threshold is 75%.

Mode Router Configuration

Example To configure the maximum number of RIP routes to 150, use the following command:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# maximum-prefix 150
```

neighbor (RIP)

Overview Use this command to specify a neighbor router. It is used for each router to which you wish to send unicast RIP updates.

Use the **no** variant of this command to stop sending unicast updates to the specific router.

Syntax

```
neighbor <ip-address>
no neighbor <ip-address>
```

Parameter	Description
<ip-address>	The IP address of a neighboring router with which the routing information will be exchanged.

Default Disabled

Mode Router Configuration

Usage Use this command to exchange nonbroadcast routing information. It can be used multiple times for additional neighbors.

The passive-interface (RIP) command disables sending routing updates on an interface. Use the `neighbor` command in conjunction with the passive-interface (RIP) to send routing updates to specific neighbors.

Example To specify the neighbor router to 1.1.1.1, use the following command:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# passive-interface vlan1
awplus(config-router)# neighbor 1.1.1.1
```

Related commands passive-interface (RIP)

network (RIP)

Overview Use this command to activate the transmission of RIP routing information on the defined network.

Use the **no** variant of this command to remove the specified network or VLAN as one that runs RIP.

Syntax

```
network {<network-address>[/<subnet-mask>]|<vlan-name>}
no network {<network-address>[/<subnet-mask>]|<vlan-name>}
```

Parameter	Description
<network-address> *[/<subnet-mask>]*	Specifies the network address to run RIP. Entering a subnet mask (or prefix length) for the network address is optional. Where no mask is entered, the device will attempt to apply a mask that is appropriate to the class (A, B, or C) of the address entered, e.g. an IP address of 10.0.0.0 will have a prefix length of 8 applied to it.
<vlan-name>	Specify a VLAN name with up to 32 alphanumeric characters to run RIP.

Default Disabled

Mode RIP Router Configuration

Usage notes Use this command to specify networks, or VLANs, to which routing updates will be sent and received. The connected routes corresponding to the specified network, or VLANs, will be automatically advertised in RIP updates. RIP updates will be sent and received within the specified network or VLAN.

Example Use the following commands to activate RIP routing updates on network 172.16.20.0/24:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# network 172.16.20.0/24
```

Related commands

show ip rip

show running-config

clear ip rip route

offset-list (RIP)

Overview Use this command to add an offset to the **in** and **out** metrics of routes learned through RIP.

Use the **no** variant of this command to remove the offset list.

Syntax

```
offset-list <access-list> {in|out} <offset> [<interface>]
no offset-list <access-list> {in|out} <offset> [<interface>]
```

Parameter	Description
<access-list>	Specifies the access-list number or names to apply. Note that you can only use standard ACLs, not extended ACLs.
`in`	Indicates the access list will be used for metrics of incoming advertised routes.
`out`	Indicates the access list will be used for metrics of outgoing advertised routes.
<offset>	`<0-16>` Specifies that the offset is used for metrics of networks matching the access list.
<interface>	An alphanumeric string that specifies the interface to match.

Default The default offset value is the metric value of the interface over which the updates are being exchanged.

Mode RIP Router Configuration

Usage Use this command to specify the offset value that is added to the routing metric. When the networks match the access list the offset is applied to the metrics. No change occurs if the offset value is zero.

Examples In this example the router examines the RIP updates being sent out from interface vlan2 and adds 5 hops to the routes matching the IP addresses specified in the access list 8. To do this, use these commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# offset-list 8 in 5 vlan2
```

Related commands access-list (extended numbered)

passive-interface (RIP)

Overview Use this command to block RIP broadcasts on the interface.

Use the **no** variant of this command to disable this function.

Syntax

```
passive-interface <interface>
no passive-interface <interface>
```

Parameter	Description
<interface>	Specifies the interface name.

Default Disabled

Mode RIP Router Configuration

Example Use the following commands to block RIP broadcasts on vlan20:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# passive-interface vlan20
```

Related commands show ip rip

recv-buffer-size (RIP)

Overview Use this command to run-time configure the RIP UDP (User Datagram Protocol) receive-buffer size to improve UDP reliability by avoiding UDP receive buffer overrun.

Use the **no** variant of this command to reset the configured RIP UDP receive-buffer size to the system default (196608 bits).

Syntax

```
recv-buffer-size <8192-2147483647>
no recv-buffer-size [<8192-2147483647>]
```

Parameter	Description
<8192-2147483647>	Specify the RIP UDP (User Datagram Protocol) buffer size value in bits.

Default 196608 bits is the system default when reset using the **no** variant of this command.

Mode Router Configuration

Examples To run-time configure the RIP UDP, use the following commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# recv-buffer-size 23456789
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no recv-buffer-size 23456789
```

redistribute (RIP)

Overview Use this command to redistribute information from other routing protocols into RIP.

Use the **no** variant of this command to disable the specified redistribution. The parameters **metric** and **routemap** may be used with the **no** variant, but have no effect.

Syntax

```
redistribute {connected|static|ospf|bgp} [metric <0-16>]
[routemap <routemap>]
```

```
no redistribute {connected|static|ospf|bgp} [metric] [routemap]
```

Parameter	Description
`routemap`	Optional. Specifies route-map that controls how routes are redistributed.
`<routemap>`	Optional. The name of the route map.
`connected`	Redistribute from connected routes.
`static`	Redistribute from static routes.
`ospf`	Redistribute from Open Shortest Path First (OSPF).
`bgp`	Redistribute from Border Gateway Protocol (BGP).
`metric <0-16>`	Optional. Sets the value of the metric that will be applied to routes redistributed into RIP from other protocols. If a value is not specified, and no value is specified using the default-metric (RIP) command, the default is one.

Default By default, the RIP metric value is set to 1.

Mode RIP Router Configuration

Example To apply the metric value 15 to static routes being redistributed into RIP, use the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# redistribute static metric 15
```

Related commands default-metric (RIP)

restart rip graceful

Overview Use this command to force the RIP process to restart, and optionally set the grace-period.

Syntax
```
restart rip graceful [grace-period <1-65535>]
```

Mode Privileged Exec

Default The default RIP grace-period is 60 seconds.

Usage notes After this command is executed, the RIP process immediately shuts down. It notifies the system that RIP has performed a graceful shutdown. Routes that have been installed into the route table by RIP are preserved until the specified grace-period expires.

When a **restart rip graceful** command is issued, the RIP configuration is reloaded from the last saved configuration. Ensure you first enter the command copy running-config startup-config.

Example To apply a restart rip graceful setting, grace-period to 100 seconds use the following commands:

```
awplus# copy running-config startup-config
awplus# restart rip graceful grace-period 100
```

rip restart grace-period

Overview Use this command to change the grace period of RIP graceful restart.

Use the **no** variant of this command to disable this function.

Syntax

```
rip restart grace-period <1-65535>
no rip restart grace-period <1-65535>
```

Mode Global Configuration

Default The default RIP grace-period is 60 seconds.

Usage notes Use this command to enable the **Graceful Restart** feature on the RIP process. Entering this command configures a grace period for RIP.

Example

```
awplus# configure terminal
awplus(config)# rip restart grace-period 200
```

route (RIP)

Overview Use this command to add a static RIP route.

Use the **no** variant of this command to remove a static RIP route.

Syntax

```
route <ip-addr/prefix-length>
no route <ip-addr/prefix-length>
```

Parameter	Description
<ip-addr/prefix-length>	The IPv4 address and prefix length.

Default No static RIP route is added by default.

Mode RIP Router Configuration

Usage notes Use this command to add a static RIP route. After adding the RIP route, the route can be checked in the RIP routing table.

Example To create a static RIP route to IP subnet 192.168.1.0/24, use the following commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# route 192.168.1.0/24
```

Related commands show ip rip

clear ip rip route

router rip

Overview Use this global command to enter Router Configuration mode to enable the RIP routing process.

Use the **no** variant of this command to disable the RIP routing process.

Syntax

```
router rip
no router rip
```

Mode Global Configuration

Example This command is used to begin the RIP routing process:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# version 1
awplus(config-router)# network 10.10.10.0/24
awplus(config-router)# network 10.10.11.0/24
awplus(config-router)# neighbor 10.10.10.10
```

Related commands network (RIP)

version (RIP)

send-lifetime

Overview Use this command to specify the time period during which the authentication key on a key chain can be sent.

Syntax

```
send-lifetime <start-date> {<end-date>|
duration <seconds>|infinite}
```

```
no send-lifetime
```

Parameter	Description	
<start-date>	Specifies the start time and date in the format: *<hh:mm:ss> <day> <month> <year>* or *<hh:mm:ss> <month> <day> <year>*, where:	
	<hh:mm:ss>	The time of the day, in hours, minutes and seconds
	<day>	<1-31> The day of the month
	<month>	The month of the year (the first three letters of the month, for example, Jan)
	<year>	<1993-2035> The year
<end-date>	Specifies the end time and date in the format: *<hh:mm:ss> <day> <month> <year>* or *<hh:mm:ss> <month> <day> <year>*, where:	
	<hh:mm:ss>	The time of the day, in hours, minutes and seconds
	<day>	<1-31> The day of the month
	<month>	The month of the year (the first three letters of the month, for example, Jan)
	<year>	<1993-2035> The year
<seconds>	<1-2147483646> Duration of the key in seconds.	
infinite	Never expires.	

Mode Keychain-key Configuration

Example The following example shows the setting of send-lifetime for key 1 on the key chain named “mychain”.

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# send-lifetime 03:03:01 Jan 3 2016
04:04:02 Dec 6 2016
```

Related commands

key

key-string

key chain

accept-lifetime

show debugging rip

Overview Use this command to display the RIP debugging status for these debugging options: nsm debugging, RIP event debugging, RIP packet debugging and RIP nsm debugging.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax
```
show debugging rip
```

Mode User Exec and Privileged Exec

Usage notes Use this command to display the debug status of RIP.

Example
```
awplus# show debugging rip
```

show ip prefix-list

Overview Use this command to display the IPv4 prefix-list entries.

Note that this command is valid for RIP and BGP routing protocols only.

Syntax

```
show ip prefix-list [<name>|detail|summary]
```

Parameter	Description
<name>	Specify the name of a prefix list in this placeholder.
`detail`	Specify this parameter to show detailed output for all IPv4 prefix lists.
`summary`	Specify this parameter to show summary output for all IPv4 prefix lists.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip prefix-list
awplus# show ip prefix-list 10.10.0.98/8
awplus# show ip prefix-list detail
```

Related commands ip prefix-list

show ip protocols rip

Overview Use this command to display RIP process parameters and statistics.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ip protocols rip
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip protocols rip
```

Output Figure 26-1: Example output from the **show ip protocols rip** command

```
Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%, next due in 12
seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing: connected static
Default version control: send version 2, receive version 2
Interface        Send  Recv   Key-chain
   vlan25          2     2
Routing for Networks:
  10.10.0.0/24
Routing Information Sources:
  Gateway          BadPackets BadRoutes  Distance Last Update
Distance: (default is 120
```

show ip rip

Overview Use this command to show RIP routes.

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

Syntax

```
show ip rip
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip rip
```

Output Figure 26-2: Example output from the **show ip rip** command

```
awplus#show ip rip
Codes: R - RIP, Rc - RIP connected, Rs - RIP static
       C - Connected, S - Static, O - OSPF, B - BGP
Network         Next Hop Metric From If    Time
C 10.0.1.0/24             1      vlan20
S 10.10.10.0/24           1      vlan20
C 10.10.11.0/24           1      vlan20
S 192.168.101.0/24        1      vlan20
R 192.192.192.0/24        1      --
```

Related commands

route (RIP)

network (RIP)

clear ip rip route

show ip rip database

Overview Use this command to display information about the RIP database.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ip rip database [full]
```

Parameter	Description
`full`	Specify the full RIP database including sub-optimal RIP routes.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip rip database
awplus# show ip rip database full
```

Related commands show ip rip

show ip rip interface

Overview Use this command to display information about the RIP interfaces. You can specify an interface name to display information about a specific interface.

Syntax

```
show ip rip interface [<interface>]
```

Parameter	Description
<interface>	The interface to display information about. For instance: `vlan2`.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip rip interface
```

timers (RIP)

Overview Use this command to adjust routing network timers.

Use the **no** variant of this command to restore the defaults.

Syntax

```
timers basic <update> <timeout> <garbage>
no timers basic
```

Parameter	Description
<update>	<5-2147483647> Specifies the period at which RIP route update packets are transmitted. The default is 30 seconds.
<timeout>	<5-2147483647> Specifies the routing information timeout timer in seconds. The default is 180 seconds. After this interval has elapsed and no updates for a route are received, the route is declared invalid.
<garbage>	<5-2147483647> Specifies the routing garbage collection timer in seconds. The default is 120 seconds.

Default Enabled

Mode RIP Router Configuration

Usage notes This command adjusts the RIP timing parameters.

The update timer is the time between sending out updates, that contain the complete routing table, to every neighboring router.

If an update for a given route has not been seen for the time specified by the timeout parameter, that route is no longer valid. However, it is retained in the routing table for a short time, with metric 16, so that neighbors are notified that the route has been dropped.

When the time specified by the garbage parameter expires the metric 16 route is finally removed from the routing table. Until the garbage time expires, the route is included in all updates sent by the router.

All the routers in the network must have the same timers to ensure the smooth operation of RIP throughout the network.

Examples To set the update timer to 30, the routing information timeout timer to 180, and the routing garbage collection timer to 120, use the following command:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# timers basic 30 180 120
```

undebug rip

Overview Use this command to disable the options set for debugging information of RIP events, packets and communication between RIP and NSM.

This command has the same effect as the **no debug rip** command.

Syntax `undebug rip {all|events|nsm|<packet>}`

Parameter	Description
`all`	Disables all RIP debugging.
`events`	Disables the logging of RIP events.
`nsm`	Disables the logging of RIP and NSM communication.
<packet>	`packet [recv|send] [detail]` Disables the debugging of RIP packets.
`recv`	Disables the logging of received packet information.
`send`	Disables the logging of sent packet information.
`detail`	Disables the logging of sent or received RIP packets.

Mode Privileged Exec

Example To disable the options set for debugging RIP information events, use the following command:

```
awplus# undebug rip packet
```

Related commands debug rip

version (RIP)

Overview Use this command to specify a RIP version used globally by the router.

Use the **no** variant of this command to restore the default version.

Syntax

```
version {1|2}
no version
```

Parameter	Description
1|2	Specifies the version of RIP processing.

Default Version 2

Mode RIP Router Configuration

Usage notes RIP can be run in version 1 or version 2 mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces.

Setting the version command has no impact on receiving updates, only on sending them. The ip rip send version command overrides the value set by the version (RIP) command on an interface-specific basis. The ip rip receive version command allows you to configure a specific interface to accept only packets of the specified RIP version. The ip rip receive version command and the ip rip send version command override the value set by this command.

Examples To specify a RIP version, use the following commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# version 1
```

Related commands

ip rip receive version

ip rip send version

show running-config

27 RIPng for IPv6 Commands

Introduction

Overview This chapter contains RIPng commands. RIPng (Routing Information Protocol next generation) is an extension of RIPv2 to support IPv6. RFC 2080 specifies RIPng. The differences between RIPv2 and RIPng are:

- RIPng does not support RIP updates authentication
- RIPng does not allow the attachment of arbitrary tags to routes
- RIPng requires the encoding of the next-hop for a set of routes

For more information, see the RIPng Feature Overview and Configuration Guide.

Command List

- "aggregate-address (IPv6 RIPng)" on page 1045
- "clear ipv6 rip route" on page 1046
- "debug ipv6 rip" on page 1047
- "default-information originate (IPv6 RIPng)" on page 1048
- "default-metric (IPv6 RIPng)" on page 1049
- "distribute-list (IPv6 RIPng)" on page 1050
- "ipv6 prefix-list" on page 1051
- "ipv6 rip metric-offset" on page 1053
- "ipv6 rip split-horizon" on page 1055
- "ipv6 router rip" on page 1056
- "neighbor (IPv6 RIPng)" on page 1057
- "offset-list (IPv6 RIPng)" on page 1058
- "passive-interface (IPv6 RIPng)" on page 1059
- "recv-buffer-size (IPv6 RIPng)" on page 1060
- "redistribute (IPv6 RIPng)" on page 1061

- "route (IPv6 RIPng)" on page 1062
- "router ipv6 rip" on page 1063
- "show debugging ipv6 rip" on page 1064
- "show ipv6 prefix-list" on page 1065
- "show ipv6 protocols rip" on page 1066
- "show ipv6 rip" on page 1067
- "show ipv6 rip database" on page 1068
- "show ipv6 rip interface" on page 1069
- "timers (IPv6 RIPng)" on page 1070
- "undebug ipv6 rip" on page 1071

aggregate-address (IPv6 RIPng)

Overview Use this command to add an aggregate route to RIPng.

Use the **no** variant of this command to remove the aggregate route from RIPng.

Syntax

```
aggregate-address <ipv6-addr/prefix-length>
no aggregate-address <ipv6-addr/prefix-length>
```

Parameter	Description
<ipv6-addr/prefix-length>	Specify the IPv6 Address in the format *X:X::X:X/Prefix-Length*. The prefix-length is a decimal integer between 1 and 128.

Mode Router Configuration

Usage notes The route will not be added to the RIPng database unless the database contains at least one route which is contained within the address range covered by the aggregate route. As soon as there are any such component routes in the RIPng database, then the following occurs:

- the aggregate route is added to the RIPng database
- all the component routes that are within the address range covered by the aggregate route are retained in the RIPng database, but are marked as suppressed routes. The aggregate route will be advertised in RIPng updates, and the component route will no longer be advertised.

Note that simply having a component route in the IPv6 route database is not a sufficient condition for the aggregate route to be included into the RIPng database. The component route(s) must be in the RIPng database before the aggregate route will be included in the RIPng database. There is no restriction on the method by which the component routes have arrived into the RIPng database, it can be by being connected RIP interfaces, by redistribution or by direct inclusion using the **route** command in router IPv6 RIP configuration mode.

Example

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# aggregate-address 2001:db8::/32
```

clear ipv6 rip route

Overview Use this command to clear specific data from the RIPng routing table.

Syntax
```
clear ipv6 rip route
{<ipv6-addr/prefix-length>|all|connected|rip|static|ospf}
```

Parameter	Description
<ipv6-addr/prefix-length>	Specify the IPv6 Address in format *X:X::X:X/Prefix-Length*. The prefix-length is a decimal integer between 1 and 128. Removes entries which exactly match this destination address from the RIPng routing table.
`connected`	Removes redistributed connected entries from RIPng routing table.
`static`	Removes redistributed static entries from the RIPng routing table.
`rip`	Removes RIPng routes from the RIPng routing table.
`ospf`	Removes redistributed OSPFv3 routes from the RIPng routing table.
`all`	Clears the entire RIPng routing table.

Mode Privileged Exec

Example
```
awplus# clear ipv6 rip route all
awplus# clear ipv6 rip route 2001:db8::/32
```

debug ipv6 rip

Overview Use this command to enable RIPng debugging and specify debugging for RIPng events, RIPng packets, or RIPng communication with NSM processes.

Use the **no** variant of this command to disable RIPng debugging.

Syntax

```
debug ipv6 rip [all|events|nsm|packet [detail]|recv
[detail]|send [detail]]
```

```
no debug ipv6 rip [all|events|nsm|packet [detail]|recv
[detail]|send [detail]]
```

Parameter	Description
`all`	Displays all RIPng debugging showing RIPng events debug information, RIPng received packets information, and RIPng sent packets information.
`events`	Displays RIPng events debug information.
`nsm`	Displays RIPng and NSM communication.
`packet`	Displays RIPng packets only.
`recv`	Displays information for received packets.
`send`	Displays information for sent packets.
`detail`	Displays detailed information for the sent or received packet.

Default RIPng debugging is disabled by default.

Mode Privileged Exec and Global Configuration

Example

```
awplus# debug ipv6 rip events
awplus# debug ipv6 rip packet send detail
awplus# debug ipv6 rip nsm
```

Related commands undebug ipv6 rip

default-information originate (IPv6 RIPng)

Overview Use this command to generate a default route into RIPng.

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

Syntax
```
default-information originate
no default-information originate
```

Default Disabled

Mode Router Configuration

Example
```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# default-information originate
```

default-metric (IPv6 RIPng)

Overview Use this command to specify the metrics to be assigned to redistributed RIPng routes.

Use the **no** variant of this command to reset the RIPng metric back to its default (1).

Syntax

```
default-metric <1-16>
no default-metric [<1-16>]
```

Parameter	Description
<1-16>	Metric value.

Default By default, the RIPng metric value is set to 1.

Mode Router Configuration

Usage This command is used with the redistribute (IPv6 RIPng) command to make the routing protocol use the specified metric value for all redistributed RIPng routes, regardless of the original protocol that the route has been redistributed from.

Note, this metric is not applied to routes that are brought into RIPng by using the **route** command in router IPv6 RIP configuration mode. This metric is, though, applied to any RIPng aggregate routes that have been brought into the RIPng database due to the presence of a component route that was redistributed into RIPng.

Also note that the default-metric is applied to routes redistributed into RIPng with no metric assignment in the routemap associated with redistribution.

Example

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# default-metric 8
```

Related commands ipv6 rip metric-offset

redistribute (IPv6 RIPng)

distribute-list (IPv6 RIPng)

Overview Use this command to filter incoming or outgoing route updates using the access-list or the prefix-list.

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

Syntax

```
distribute-list [<access-list>|prefix <prefix-list-name>]
[in|out] [<interface>]
```

```
no distribute-list [<access-list>|prefix <prefix-list-name>]
[in|out] [<interface>]
```

```
no distribute-list [prefix <prefix-list-name>] [in|out]
[<interface>]
```

Parameter	Description
<access-list>	Specifies the IPv6 access-list number or name to use.
<prefix-list-name>	Filter prefixes in routing updates. Specify the name of the IPv6 prefix-list to use.
<interface>	The interface for which distribute-list applies. For instance: `vlan2`.
`in`	Filter incoming routing updates.
`out`	Filter outgoing routing updates.

Default Disabled

Mode Router Configuration

Usage notes Filter out incoming or outgoing route updates using the access-list or the prefix-list. If you do not specify the name of the interface, the filter is applied to all the interfaces.

Example To filter incoming or outgoing route updates, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# distribute-list prefix myfilter in vlan2
```

Related commands ipv6 access-list extended (named)

ipv6 nd prefix

ipv6 prefix-list

Overview Use this command to create an IPv6 prefix list or an entry in an existing prefix list.

Use the **no** variant of this command to delete a whole prefix list, a prefix list entry, or a description.

Syntax

```
ipv6 prefix-list <list-name> [seq <1-429496725>] {deny|permit} {any|<ipv6-prefix>} [ge <0-128>] [le <0-128>]
ipv6 prefix-list <list-name> description <text>
no ipv6 prefix-list <list-name> [seq <1-429496725>]
no ipv6 prefix-list <list-name> [description <text>]
```

Parameter	Description
`<list-name>`	Specifies the name of a prefix list.
`seq <1-429496725>`	Sequence number of the prefix list entry.
`deny`	Specifies that the prefixes are excluded from the list.
`permit`	Specifies that the prefixes are included in the list.
`<ipv6-prefix>`	Specifies the IPv6 prefix and prefix length in hexadecimal in the format X:X::X:X/M.
`any`	Any prefix match. Same as ::0/0 le 128.
`ge <0-128>`	Specifies the minimum prefix length to be matched.
`le <0-128>`	Specifies the maximum prefix length to be matched.
`description`	Prefix list specific description.
`<text>`	Up to 80 characters of text description of the prefix list.

Mode Global Configuration

Usage notes When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the **seq** parameter and place common permits or denials towards the top of the list. If you do not use the **seq** parameter, the sequence values are generated in a sequence of 5.

The parameters **ge** and **le** specify the range of the prefix lengths to be matched. The parameters **ge** and **le** are only used if an ip-prefix is stated. When setting these parameters, set the **le** value to be less than 128, and the **ge** value to be less than or equal to the **le** value and greater than the ip-prefix mask length.

Prefix lists implicitly exclude prefixes that are not explicitly permitted in the prefix list. This means if a prefix that is being checked against the prefix list reaches the end of the prefix list without matching a permit or deny, this prefix will be denied.

Example To check the first 32 bits of the prefix 2001:db8:: and that the subnet mask must be greater than or equal to 34 and less than or equal to 40, enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 prefix-list mylist seq 12345 permit
2001:db8::/32 ge 34 le 40
```

Related commands

match ipv6 address

show ipv6 prefix-list

show running-config ipv6 prefix-list

ipv6 rip metric-offset

Overview Use this command to increment the metric value on incoming routes for a specified interface. This command can be used to artificially inflate the metric value for routes learned on the specified interface. Routes learned on the specified interface are only used if the routes to the same destination with a lower metric value in the routing table are down.

Use the **no** variant of this command to reset the metric value on incoming routes to the default value (1). You can set the metric value for redistributed routes with default-metric (IPv6 RIPng) and redistribute (IPv6 RIPng) commands in Router Configuration mode.

Syntax

```
ipv6 rip metric-offset <1-16>
no ipv6 rip metric-offset <1-16>
```

Parameter	Description
<1-16>	Specify an increment to the metric value on an incoming route. The metric value for RIPng routes is the hop count for the route.

Default The default RIPng metric value is 1.

Mode Interface Configuration for a VLAN interface only.

Usage notes When a RIPng route is received on a VLAN interface, the metric value for the interface set by this command is added to the metric value of the route in the routing table. Note this command only increments the metric for incoming routes on a specified interface. Increasing the metric value for a VLAN interface increases the metric value of routes received on that VLAN interface. This changes the route selected from the routing table.

The RIPng metric is the hop count. At regular intervals of the routing update timer (which has a default value of 30 seconds), and at the time of change in the topology, the RIPng router sends update messages to other routers. The listening routers update their route table with the new route, and increase the metric value of the path by one (referred to as a hop count). The router recognizes the IPv6 address advertising router as the next hop, then sends the routing updates to other routers. A maximum allowable hop count is 15. If a router reaches a metric value of 16 or more, the destination is identified as unreachable.

For information about how AlliedWare Plus adds routes, see the "Route Selection" Feature Overview and Configuration Guide. See also the default-metric (IPv6 RIPng)and redistribute (IPv6 RIPng) commands to specify the metric for redistributed RIPng routes.

Examples

To increment the metric-offset on the VLAN interface vlan2, enter the below commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# exit
awplus(config)# interface vlan2
awplus(config-if)# ipv6 rip metric-offset 1
```

To reset the metric-offset on the VLAN interface `vlan2` to the default value, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 rip metric-offset 1
```

Validation Commands

show running-config

Related commands

default-metric (IPv6 RIPng)

ipv6 rip split-horizon

Overview Use this command to perform the split-horizon action on the interface. The default is split-horizon with poisoned reverse.

Use the **no** variant of this command to disable this function.

Syntax

```
ipv6 rip split-horizon [poisoned]
no ipv6 rip split-horizon
```

Parameter	Description
`split-horizon`	Perform split-horizon without poisoned reverse
`poisoned`	Performs split-horizon with poisoned reverse.

Default Split-horizon with poisoned reverse is the default.

Mode Interface Configuration for a VLAN interface only.

Usage notes Use this command to avoid including routes in updates sent to the same gateway from which they were learned. Using the **split horizon** command omits routes learned from one neighbor, in updates sent to that neighbor. Using the **poisoned** parameter with this command includes such routes in updates, but sets their metrics to infinity. Thus, advertising that these routes are not reachable.

Examples To perform split-horizon with poisoned reverse on the VLAN interface `vlan2`, enter the below commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# exit
awplus(config)# interface vlan2
awplus(config-if)# ipv6 rip split-horizon poisoned
```

To disable split-horizon on the VLAN interface `vlan2`, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 rip split-horizon
```

Validation Commands show running-config

ipv6 router rip

Overview Use this command to enable RIPng routing on an interface.

Use the **no** variant of this command to disable RIPng routing on an interface.

Syntax

```
ipv6 router rip
no ipv6 router rip
```

Default RIPng routing is disabled by default.

Mode Interface Configuration for a VLAN interface only.

Usage notes This command can only be configured on VLAN interfaces.

Examples To enable RIPng routing on the VLAN interface vlan2, enter the below commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# exit
awplus(config)# interface vlan2
awplus(config-if)# ipv6 router rip
```

To disable RIPng routing on the VLAN interface vlan2, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 router rip
```

neighbor (IPv6 RIPng)

Overview Use this command to specify a neighbor router.

Use the **no** variant of this command to disable the specific router.

Syntax

```
neighbor <ipv6-link-local-addr> <interface>
no neighbor <ipv6-link-local-addr> <interface>
```

Parameter	Description
<ipv6-link-local-addr>	Specify the link-local IPv6 address (in the format *X:X::X:X*) of a neighboring router to exchange routing information with.
<interface>	The interface. For instance: `vlan2`.

Mode Router Configuration

Usage Use this command to exchange non broadcast routing information. It can be used multiple times for additional neighbors.

The passive-interface (IPv6 RIPng) command disables sending routing updates on an interface. Use the `neighbor` command in conjunction with the passive-interface (IPv6 RIPng) command to send routing updates to specific neighbors.

Examples

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# neighbor 2001:db8:1::1 vlan2
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# no neighbor 2001:db8:1::1 vlan2
```

Related commands passive-interface (IPv6 RIPng)

offset-list (IPv6 RIPng)

Overview Use this command to add an offset to in and out metrics to routes learned through RIPng.

Use the **no** variant of this command to remove an offset list.

Syntax

```
offset-list {<access-list-number>|<access-list-name>} {in|out} <offset> [<interface>]
```

```
no offset-list {<access-list-number>|<access-list-name>} {in|out} <offset> [<interface>]
```

Parameter	Description
<access-list-number>	Specify an access-list number to apply to an offset-list.
<access-list-name>	Specify and access-list name to apply to an offset-list.
`in`	Indicates the access-list will be used for metrics of incoming advertised routes
`out`	Indicates the access-list will be used for metrics of outgoing advertised routes
<offset>	`<0-16>` Specifies that the offset is used for metrics of networks matching the access-list
<interface>	The interface to match. For instance: `vlan2`.

Default The default offset value is the metric value of the interface over which the updates are being exchanged.

Mode Router Configuration

Usage notes Use this command to specify the offset value that is added to the routing metric. When the networks match the access list the offset is applied to the metrics. No change occurs if the offset value is zero.

Example In this example the router examines the RIPng updates being sent out from interface `vlan2` and adds `8` hops to the routes matching the ip addresses specified in the access list `2`.

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# offset-list mylist in 8 vlan2
```

passive-interface (IPv6 RIPng)

Overview Use this command to enable suppression of routing updates on an interface.

Use the **no** variant of this command to disable this function.

Syntax

```
passive-interface <interface>
no passive-interface <interface>
```

Parameter	Description
<interface>	The interface. For instance: `vlan2`.

Default Disabled

Mode Router Configuration

Examples To enable suppression of routing updates, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# passive-interface vlan2
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# no passive-interface vlan2
```

recv-buffer-size (IPv6 RIPng)

Overview Use this command to configure the RIPng UDP (User Datagram Protocol) receive-buffer size. This should improve UDP reliability by avoiding UDP receive buffer overruns.

Use the **no** variant of this command to unset the configured RIPng UDP receive-buffer size and set it back to the system default of 196608 bits.

Syntax

```
recv-buffer-size <8192-2147483647>
no recv-buffer-size [<8192-2147483647>]
```

Default The RIPng UDP receive-buffer-size is 196608 bits by default, and is reset to the default using the **no** variant of this command.

Mode Router Configuration

Examples To configure the RIPng UPD, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# recv-buffer-size 23456789
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# no recv-buffer-size 23456789
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# no recv-buffer-size
```

redistribute (IPv6 RIPng)

Overview Use this command to redistribute information from other routing protocols into RIPng.

Use the **no** variant of this command to disable the specified redistribution. The parameters **metric** and **routemap** may be used on this command, but have no effect.

Syntax

```
redistribute {connected|static|ospf} [metric <0-16>] [route-map
<route-map>]
```

```
no redistribute {connected|static|ospf} [metric <0-16>]
[route-map <route-map>]
```

Parameter	Description
<0-16>	Optional. Specifies the metric value to be used when redistributing information. If a value is not specified, and no value is specified using the default-metric (IPv6 RIPng) command, the default is one.
<route-map>	Optional. Specifies route-map to be used to redistribute information.
`connected`	Redistribute from connected routes.
`static`	Redistribute from static routes.
`ospf`	Redistribute from Open Shortest Path First (OSPF).

Default By default, the RIPng metric value is set to 1.

Mode Router Configuration

Example To redistribute information from other routing protocols into RIPng, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# redistribute static route-map mymap
awplus(config-router)# redistribute static metric 8
```

Related commands default-metric (IPv6 RIPng)

route (IPv6 RIPng)

Overview Use this command to configure static RIPng routes.

Use the **no** variant of this command to disable this function.

Syntax

```
route <ipv6-addr/prefix-length>
no route <ipv6-addr/prefix-length>
```

Parameter	Description
<ipv6-addr/prefix-length>	Specify the IPv6 Address in format *X:X::X:X/Prefix-Length*. The prefix-length is a decimal integer between 1 and 128.

Mode Router Configuration

Usage notes Use this command to add a static RIPng route. After adding the RIPng route, the route can be checked in the RIPng routing table.

Example To configure static RIPng routes, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# route 2001:db8::1/64
```

Related commands show ipv6 rip

clear ipv6 rip route

router ipv6 rip

Overview Use this global command to enter Router Configuration mode to enable a RIPng routing process.

Use the **no** variant of this command to disable the RIPng routing process.

Syntax

```
router ipv6 rip
no router ipv6 rip
```

Mode Global Configuration

Example To enable a RIPng routing process, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)#
```

show debugging ipv6 rip

Overview Use this command to see what debugging is turned on for RIPng options such as: nsm debugging, RIPng event debugging, RIPng packet debugging, and RIPng nsm debugging.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show debugging ipv6 rip
```

Mode User Exec and Privileged Exec

Usage notes Use this command to display the debug status of RIPng.

Example To display the RIPng debugging status, use the following command:

```
awplus# show debugging ipv6 rip
```

show ipv6 prefix-list

Overview Use this command to display the prefix-list entries.

Note that this command is valid for RIPng and BGP4+ routing protocols only.

Syntax

```
show ipv6 prefix-list [<name>|detail|summary]
```

Parameter	Description
<name>	Specify the name of an individual IPv6 prefix list.
`detail`	Specify this parameter to show detailed output for all IPv6 prefix lists.
`summary`	Specify this parameter to show summary output for all IPv6 prefix lists.

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 prefix-list
awplus# show ipv6 prefix-list 10.10.0.98/8
awplus# show ipv6 prefix-list detail
```

Related commands ipv6 prefix-list

show ipv6 protocols rip

Overview Use this command to display RIPng process parameters and statistics.

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

Syntax

```
show ipv6 protocols rip
```

Mode User Exec and Privileged Exec

Example To display RIPng process parameters and statistics, use the following command:

```
awplus# show ipv6 protocols rip
```

Output

```
awplus#show ipv6 protocols rip
Routing Protocol is "RIPng"
  Sending updates every 30 seconds with +/-5 seconds, next due
in 6 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribute metric is 1
  Redistributing:
  Interface
    vlan3
  Routing for Networks:
    fe80::200:cdff:fe27:c086 vlan1
```

show ipv6 rip

Overview Use this command to show RIPng routes.

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

Syntax

```
show ipv6 rip
```

Mode User Exec and Privileged Exec

Example To display RIPng routes, use the following command:

```
awplus# show ipv6 rip
```

Output

```
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP
aggregated, Rcx - RIP connect suppressed, Rsx - RIP static
suppressed, C - Connected, S - Static, O - OSPF, B - BGP

   Network           Next Hop         If     Met Tag   Time

R  2001:db8:1::/48   2001:db8:2::/48  vlan3   3   0    02:28
C  2001:db8:3::/48   ::               vlan2   1   0
Ra 2001:db8:4::/48                    --      1   0
Rs 2001:db8:5::/48   2001:db8:1::/48  vlan3   3   0    02:32
Cs 2001:db8:6::/48   ::               vlan3   1   0
```

Related commands show ipv6 rip database

show ipv6 rip database

Overview Use this command to display information about the RIPng database.

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

Syntax

```
show ipv6 rip database [full]
```

Parameter	Description
`full`	Display all IPv6 RIPng full database entries including sub-optimal routes.

Mode User Exec and Privileged Exec

Example To display information about the RIPng database, use the following command:

```
awplus# show ipv6 rip database
```

Output

```
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP
aggregated, Rcx - RIP connect suppressed, Rsx - RIP static
suppressed, C - Connected, S - Static, O - OSPF, B - BGP

   Network            Next Hop          If     Met Tag   Time

R  2001:db8:1::/48    2001:db8:2::/48   vlan3   3   0    02:28
C  2001:db8:3::/48    ::                vlan2   1   0
Ra 2001:db8:4::/48                      --      1   0
Rs 2001:db8:5::/48    2001:db8:1::/48   vlan3   3   0    02:32
Cs 2001:db8:6::/48    ::                vlan3   1   0
```

Related commands show ipv6 rip

show ipv6 rip interface

Overview Use this command to display information about the RIPng interfaces. You can specify an interface name to display information about a specific interface.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 rip interface [<interface>]
```

Parameter	Description
<interface>	The interface to display information about. For instance: `vlan2`.

Mode User Exec and Privileged Exec

Example To display RIPng interface information, use the following command:

```
awplus# show ipv6 rip interface
```

Output

```
lo is up, line protocol is up
RIPng is not enabled on this interface
vlan1 is up, line protocol is up
RIPng is not enabled on this interface
vlan2 is down, line protocol is down
RIPng is not enabled on this interface
vlan3 is up, line protocol is up
Routing Protocol: RIPng
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
IP interface address:
2001:db8:1::1/64
2001:db8:1::2/64
```

timers (IPv6 RIPng)

Overview Use this command to adjust the RIPng routing network timers.

Use the **no** variant of this command to restore the defaults.

Syntax

```
timers basic <update> <timeout> <garbage>
no timers basic
```

Parameter	Description
<update>	<5-2147483647> Specifies the RIPng routing table update timer in seconds. The default is 30 seconds.
<timeout>	<5-2147483647> Specifies the RIPng routing information timeout timer in seconds. The default is 180 seconds. After this interval has elapsed and no updates for a route are received, the route is declared invalid.
<garbage>	<5-2147483647> Specifies the RIPng routing garbage collection timer in seconds. The default is 120 seconds.

Default The default RIPng routing table update timer default is 30 seconds, the default RIPng routing information timeout timer is 180 seconds, and the default RIPng routing garbage collection timer is 120 seconds. The **no** variant of this command restores the default RIPng routing timers.

Mode Router Configuration

Example To adjust the RIPng routing network timers, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# timers basic 30 180 120
```

undebug ipv6 rip

Overview Use this command to disable debugging options of RIPng events, RIPng packets, and communication between RIPng and NSM processes.

Syntax

```
undebug ipv6 rip [all|events|nsm|packet [recv|send][detail]]
```

Parameter	Description
`all`	Disables all RIPng debugging.
`events`	Disable the display of RIPng events information.
`nsm`	Disable the display of RIPng and NSM communication.
`packet`	Disable debugging of specified RIPng packets only.
`recv`	Disable the display of information for received packets.
`send`	Disable the display of information for sent packets.
`detail`	Disable the display of detailed information for sent or received packets.

Mode Privileged Exec and Global Configuration

Example To disable debugging options, use the following command:

```
awplus# undebug ipv6 rip events
awplus# undebug ipv6 rip all
awplus# undebug ipv6 rip packet send
awplus# undebug ipv6 rip packet recv detail
```

Related commands debug ipv6 rip

28 OSPF Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure OSPF. For more information, see the OSPF Feature Overview and Configuration Guide.

Command List

- "area default-cost" on page 1075
- "area authentication" on page 1076
- "area filter-list" on page 1077
- "area nssa" on page 1078
- "area range" on page 1080
- "area stub" on page 1082
- "area virtual-link" on page 1083
- "auto-cost reference bandwidth" on page 1086
- "bandwidth" on page 1088
- "capability opaque" on page 1089
- "capability restart" on page 1090
- "clear ip ospf process" on page 1091
- "compatible rfc1583" on page 1092
- "debug ospf events" on page 1093
- "debug ospf ifsm" on page 1094
- "debug ospf lsa" on page 1095
- "debug ospf nfsm" on page 1096
- "debug ospf nsm" on page 1097
- "debug ospf packet" on page 1098

- "debug ospf route" on page 1099
- "default-information originate" on page 1100
- "default-metric (OSPF)" on page 1101
- "distance (OSPF)" on page 1102
- "distribute-list (OSPF)" on page 1104
- "enable db-summary-opt" on page 1107
- "host area" on page 1108
- "ip ospf authentication" on page 1109
- "ip ospf authentication-key" on page 1110
- "ip ospf cost" on page 1111
- "ip ospf database-filter" on page 1112
- "ip ospf dead-interval" on page 1113
- "ip ospf disable all" on page 1114
- "ip ospf hello-interval" on page 1115
- "ip ospf message-digest-key" on page 1116
- "ip ospf mtu" on page 1118
- "ip ospf mtu-ignore" on page 1119
- "ip ospf network" on page 1120
- "ip ospf priority" on page 1121
- "ip ospf resync-timeout" on page 1122
- "ip ospf retransmit-interval" on page 1123
- "ip ospf transmit-delay" on page 1124
- "max-concurrent-dd" on page 1125
- "maximum-area" on page 1126
- "neighbor (OSPF)" on page 1127
- "network area" on page 1128
- "ospf abr-type" on page 1130
- "ospf restart grace-period" on page 1131
- "ospf restart helper" on page 1132
- "ospf router-id" on page 1134
- "overflow database" on page 1135
- "overflow database external" on page 1136
- "passive-interface (OSPF)" on page 1137
- "redistribute (OSPF)" on page 1138
- "restart ospf graceful" on page 1140

- "router ospf" on page 1141
- "router-id" on page 1142
- "show debugging ospf" on page 1143
- "show ip ospf" on page 1144
- "show ip ospf border-routers" on page 1147
- "show ip ospf database" on page 1148
- "show ip ospf database asbr-summary" on page 1150
- "show ip ospf database external" on page 1151
- "show ip ospf database network" on page 1153
- "show ip ospf database nssa-external" on page 1154
- "show ip ospf database opaque-area" on page 1156
- "show ip ospf database opaque-as" on page 1157
- "show ip ospf database opaque-link" on page 1158
- "show ip ospf database router" on page 1159
- "show ip ospf database summary" on page 1161
- "show ip ospf interface" on page 1164
- "show ip ospf neighbor" on page 1165
- "show ip ospf route" on page 1167
- "show ip ospf virtual-links" on page 1168
- "show ip protocols ospf" on page 1169
- "summary-address" on page 1170
- "timers spf exp" on page 1171
- "undebug ospf events" on page 1172
- "undebug ospf ifsm" on page 1173
- "undebug ospf lsa" on page 1174
- "undebug ospf nfsm" on page 1175
- "undebug ospf nsm" on page 1176
- "undebug ospf packet" on page 1177
- "undebug ospf route" on page 1178

area default-cost

Overview This command specifies a cost for the default summary route sent into a stub or NSSA area.

The **no** variant of this command removes the assigned default-route cost.

Syntax

```
area <area-id> default-cost <0-16777215>
no area <area-id> default-cost
```

Parameter	Description	
<area-id>	The OSPF area that you are specifying the default summary route cost for. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format.	
	<ip-addr>	OSPF Area ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295>	OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.	
default-cost	Indicates the cost for the default summary route used for a stub or NSSA area. Default: **1**	

Mode Router Configuration

Usage The default-cost option provides the metric for the summary default route, generated by the area border router, into the NSSA or stub area. Use this option only on an area border router that is attached to the NSSA or stub area. Refer to the RFC 3101 for information on NSSA.

Example To set the default cost to 10 in area 1 for the OSPF instance 100, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# area 1 default-cost 10
```

Related commands

area nssa

area stub

area authentication

Overview Use this command to enable authentication for an OSPF area. Specifying the area authentication sets the authentication to Type 1 authentication or the Simple Text password authentication (details in RFC 2328).

The **no** variant of this command removes the authentication specification for an area.

Syntax

```
area <area-id> authentication [message-digest]
no area <area-id> authentication
```

Parameter	Description	
<area-id>	The OSPF area that you are enabling authentication for. This can be entered in either dotted decimal format or normal decimal format.	
	<ip-addr>	OSPF Area ID expressed in IPv4 address, entered in the form A.B.C.D.
	<0-4294967295>	OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area OSPF Area ID.	
message-digest	Enables MD5 authentication in the OSPF area.	

Default By default, no authentication occurs.

Mode Router Configuration

Usage All OSPF packets transmitted in this **area** must have the same password in their OSPF header. This ensures that only routers that have the correct password may join the routing domain.

Give all routers that are to communicate with each other through OSPF the same authentication password.

Use the ip ospf authentication-key command to specify a Simple Text password. Use the ip ospf message-digest-key command to specify MD5 password.

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# area 1 authentication
```

Related commands ip ospf authentication

ip ospf message-digest-key

area filter-list

Overview This command configures filters to advertise summary routes on Area Border Routers (ABR).

This command is used to suppress particular intra-area routes from/to an area to/from the other areas. You can use this command in conjunction with either the access-list or the prefix-list command.

The **no** variant of this command removes the filter configuration.

Syntax

```
area <area-id> filter-list access <access-list> {in|out}
area <area-id> filter-list prefix <prefix-list>} {in|out}
no area <area-id> filter-list access <access-list> {in|out}
no area <area-id> filter-list prefix <prefix-list>} {in|out}
```

Parameter	Description	
<area-id>	The OSPF area that you are configuring the filter for. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format.	
	<ip-addr>	OSPF Area ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295>	OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.	
access	Use access-list to filter summary.	
<access-list>	Name of an access-list.	
prefix	Use prefix-list to filter summary.	
<prefix-list>	Name of a prefix-list.	
in	Filter routes from the other areas to this area.	
out	Filter routes from this area to the other areas.	

Mode Router Configuration

Example To configure filters to advertise summary routes, use the following commands:

```
awplus# configure terminal
awplus(config)# access-list 1 deny 172.22.0.0
awplus(config)# router ospf 100
awplus(config-router)# area 1 filter-list access 1 in
```

area nssa

Overview This command sets an area as a Not-So-Stubby-Area (NSSA). By default, no NSSA area is defined.

Use this command to simplify administration if you are connecting a central site using OSPF to a remote site that is using a different routing protocol. You can extend OSPF to cover the remote connection by defining the area between the central router and the remote router as an NSSA.

There are no external routes in an OSPF stub area, so you cannot redistribute from another protocol into a stub area. A NSSA allows external routes to be flooded within the area. These routes are then leaked into other areas. Although, the external routes from other areas still do not enter the NSSA. You can either configure an area to be a stub area or an NSSA, not both.

The **no** variant of this command removes this designation.

Syntax

```
area <area-id> nssa [default-information-originate <metric> |
no-redistribution | no-summary | translator-role <role> ]
```

```
no area <area-id> nssa [default-information-originate |
no-redistribution | no-summary | translator-role ]
```

Parameter	Description	
<area-id>	The OSPF area that you are configuring as an NSSA. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format.	
	<ip-addr>	OSPF Area ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295>	OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.	
`default-information-originate`	Originate Type-7 default LSA into NSSA.	
<metric>	The external or internal metric. Specify the following:	
	`metric`*<0-1677721 4>*	The metric value.
	`metric-type`*<1-2>*	External metric type.
`no-redistribution`	Do not redistribute external route into NSSA.	
`no-summary`	Do not inject inter-area route into NSSA.	
`translator-role`	Specify NSSA-ABR translator-role.	

Parameter	Description	
<role>	The role type. Specify one of the following keywords:	
	`always`	Router always translate NSSA-LSA to Type-5 LSA.
	`candidate`	Router may translate NSSA-LSA to Type-5 LSA if it is elected.
	`never`	Router never translate NSSA-LSA.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# area 0.0.0.51 nssa
awplus(config-router)# area 3 nssa translator-role candidate
no-redistribution default-information-originate metric 34
metric-type 2
```

Related commands area default-cost

area range

Overview Use this command to summarize OSPF routes at an area boundary, configuring an IPv4 address range which consolidates OSPF routes. By default, this feature is not enabled.

A summary route created by this command is then advertised to other areas by the Area Border Routers (ABRs). In this way, routing information is condensed at area boundaries and outside the area so that routes are exchanged between areas in an efficient manner.

If the network numbers in an area are arranged into sets of contiguous routes, the ABRs can be configured to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

Use the cost parameter to specify a metric that will be advertised in the summary Link State Advertisement (LSA), rather than relying on the standard method to calculate the metric for the LSA.

The **no** variant of this command disables this function and restores default behavior.

Syntax

```
area <area-id> range <ip-addr/prefix-length> [advertise] [cost <0-16777215>]
area <area-id> range <ip-addr/prefix-length> not-advertise
no area <area-id> range <ip-addr/prefix-length>
```

Parameter	Description	
<area-id>	The OSPF area that you summarizing the routes for. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format.	
	<ip-addr>	OSPF Area ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295>	OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.	
<ip-addr/prefix-length>	The area range prefix and length.	
advertise	Advertise this range as a summary route into other areas.	

Parameter	Description
`not-advertise`	Does not advertise this range.
`cost`	Optionally override the metric that would normally be calculated for this summary with a user-defined cost to be advertised for this summary LSA. Specify the metric to be advertised for this route in the range 0-16777215.

Default The area range is not configured by default. The area range is advertised if it is configured.

Mode Router Configuration

Usage notes You can configure multiple ranges on a single area with multiple instances of this command, so OSPF summarizes addresses for different sets of IPv4 address ranges.

Ensure OSPF IPv4 routes exist in the area range for advertisement before using this command.

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# area 1 range 192.16.0.0/16
awplus(config-router)# area 1 range 203.18.0.0/16 cost 70
```

To remove a cost configured on an area range, re-enter the area range without the optional cost parameter. This will set the metric calculation back to the default algorithm.

```
awplus(config-router)# area 1 range 207.14.0.0/16 cost 35
awplus(config-router)# area 1 range 207.14.0.0/16
```

Command changes Version 5.5.0-0.1: parameter **cost** added

area stub

Overview This command defines an OSPF area as a stub area. By default, no stub area is defined.

Use this command when routers in the area do not require learning about summary LSAs from other areas. You can define the area as a totally stubby area by configuring the Area Border Router of that area using the **area stub no-summary** command.

There are two stub area router configuration commands: the **area stub** and **area default-cost** commands. In all routers attached to the stub area, configure the area by using the **area stub** command. For an area border router (ABR) attached to the stub area, also use the **area default-cost** command.

The **no** variant of this command removes this definition.

Syntax

```
area <area-id>  stub [no-summary]
no area <area-id> stub [no-summary]
```

Parameter	Description	
<area-id>	The OSPF area that you are configuring as a stub area. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format. For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.	
	<ip-addr>	OSPF Area ID expressed in IPv4 address in the format A.B.C.D.
	<0-4294967295>	OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.	
no-summary	Stops an ABR from sending summary link advertisements into the stub area.	

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# area 1 stub
```

Related commands area default-cost

area virtual-link

Overview This command configures a link between two backbone areas that are physically separated through other non-backbone areas.

In OSPF, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection.

The **no** variant of this command removes the virtual link.

Syntax

```
area <area-id> virtual-link <ip-addr> [<auth-key>|<msg-key>]

no area <area-id>  virtual-link <ip-addr>[<auth-key>|<msg-key>]

area <area-id>  virtual-link <ip-addr> authentication
[message-digest|null] [<auth-key>|<msg-key>]

no area <area-id>  virtual-link <ip-addr> authentication
[message-digest|null] [<auth-key>|<msg-key>]

area <area-id>  virtual-link <ip-addr> [authentication]
[dead-interval <1-65535>] [hello-interval <1-65535>]
[retransmit-interval <1-3600>] [transmit-delay <1-3600>]

no area <area-id>  virtual-link <ip-addr>[authentication]
[dead-interval] [hello-interval] [retransmit-interval]
[transmit-delay]
```

Parameter	Description	
<area-id>	The area ID of the transit area that the virtual link passes through. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format.	
	<ip-addr>	OSPF Area ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295>	OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.	
<ip-address>	The OSPF router ID of the virtual link neighbor.	
<auth-key>	Specifies the password used for this virtual link. Use the format: **authentication-key***<pswd-short>*	
	<pswd-short>	An 8 character password.
<msg-key>	Specifies a message digest key using the MD5 encryption algorithm. Use the following format: **message-digest-key***<1-255>* md5 *<pswd-long>*	
	<1-255>	The key ID.
	<pswd-long>	Authentication password of 16 characters.
`authentication`	Enables authentication on this virtual link.	

Parameter	Description	
`message-digest`	Use message-digest authentication.	
`null`	Use null authentication to override password or message digest.	
`dead-interval`	If no packets are received from a particular neighbor for dead-interval seconds, the router considers that neighboring router as being off-line. Default: 40 seconds	
	<1-65535>	The number of seconds in the interval.
`hello-interval`	The interval the router waits before it sends a hello packet. Default: 10 seconds	
	<1-65535>	The number of seconds in the interval.
`retransmit-interval`	The interval the router waits before it retransmits a packet. Default: 5 seconds	
	<1-3600>	The number of seconds in the interval.
`transmit-delay`	The interval the router waits before it transmits a packet. Default: 1 seconds	
	<1-3600>	The number of seconds in the interval.

Mode Router Configuration

Usage notes You can configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these two routers, joined by a virtual link, as if they were connected by an unnumbered point-to-point network. To configure a virtual link, you require:

- The transit area ID, i.e. the area ID of the non backbone area that the two backbone routers are both connected to.
- The corresponding virtual link neighbor's router ID. To see the router ID use the show ip ospf command.

Configure the **hello-interval** to be the same for all routers attached to a common network. A short **hello-interval** results in the router detecting topological changes faster but also an increase in the routing traffic.

The **retransmit-interval** is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The **transmit-delay** is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet, are incremented by this amount. Set the **transmit-delay** to be greater than zero. Also, take into account the transmission and propagation delays for the interface.

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# area 1 virtual-link 10.10.11.50 hello 5
dead 10
```

Related commands

area authentication

show ip ospf

show ip ospf virtual-links

auto-cost reference bandwidth

Overview This command controls how OSPF calculates default metrics for the interface.

Use the **no** variant of this command to assign cost based only on the interface bandwidth.

Syntax

```
auto-cost reference-bandwidth <1-4294967>
no auto-cost reference-bandwidth
```

Parameter	Description
<1-4294967>	The reference bandwidth in terms of Mbits per second (Mbps).

Default 1000 Mbps

Usage notes By default, OSPF calculates the OSPF metric for an interface by dividing the reference bandwidth by the interface bandwidth. The default for the reference bandwidth is 1000 Mbps. As a result, if this default is used, there is very little difference between the metrics applied to interfaces of increasing bandwidth beyond 1000 Mbps.

The auto-cost command is used to alter this reference bandwidth in order to give a real difference between the metrics of high bandwidth links of differing bandwidths. In a network that has multiple links with high bandwidths, specify a larger reference bandwidth value to differentiate the costs on those links.

Cost is calculated by dividing the reference bandwidth (Mbps) by the layer 3 interface (Switched Virtual Interface (SVI), Loopback or Ethernet interface) bandwidth. Interface bandwidth may be altered by using the bandwidth command as the SVI does not auto detect the bandwidth based on the speed of associated switch ports.

When the reference bandwidth calculation results in a cost integer greater than 1 but contains a fractional value (value after the decimal point), the result rounds down to the nearest integer. The following example shows how the cost is calculated.

The reference bandwidth is 1000 Mbps and the interface bandwidth is 7 Mbps.

Calculation = 1000/7

Calculation result = 142.85 (integer of 142, fractional value of 0.85)

Result after rounding down to the nearest integer = 142 (Interface cost is 142)

When the reference bandwidth calculation results in a cost less than 1, it is rounded up to the nearest integer which is 1. The following example shows how the cost is calculated.

The reference bandwidth is 1000 Mbps and the interface bandwidth is 10000 Mbps.

Calculation = 1000/10000

Calculation result = 0.1

Result after rounding up to the nearest integer = 1 (Interface cost is 1)

The auto-cost reference bandwidth value should be consistent across all OSPF routers in the OSPF process.

Note that using the ip ospf cost command on a layer 3 interface will override the cost calculated by this command.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# auto-cost reference-bandwidth 1000
```

Related commands ip ospf cost

bandwidth

Overview Use this command to specify the maximum bandwidth to be used for each VLAN interface. The bandwidth value is in bits per second. OSPF uses this to calculate metrics for the VLAN interface.

The **no** variant of this command removes any applied bandwidth value and replaces it with a value equal to the lowest port speed within that VLAN.

Syntax

```
bandwidth  <bandwidth-setting>
no bandwidth
```

Parameter	Description
<bandwidth-setting>	Sets the bandwidth for the interface. Enter a value in the range 1 to 10000000000 bits per second. Note that to avoid entering many zeros, you can add k, m, or g to internally add 3, 6 or 9 zeros to the number entered. For example entering 1k is the same as entering 1000.

Mode Interface Configuration for a VLAN interface.

Example To set the bandwidth on VLAN2 to be 1 Mbps, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# bandwidth 1000000
```

Or

```
awplus(config-if)# bandwidth 1m
```

Related commands show running-config access-list

show interface

capability opaque

Overview This command enables opaque-LSAs. Opaque-LSAs are Type 9, 10 and 11 LSAs that deliver information used by external applications.

Use the **no** variant of this command to disable opaque-LSAs.

Syntax

```
capability opaque
no capability opaque
```

Default By default, opaque-LSAs are enabled.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# no capability opaque
```

capability restart

Overview This command enables OSPF Graceful Restart or restart signaling features. By default, this is enabled.

Use the **no** variant of this command to disable OSPF Graceful Restart and restart signaling features.

Syntax

```
capability restart [graceful|signaling]
no capability restart
```

Parameter	Description
`graceful`	Enable graceful OSPF restart.
`signaling`	Enable OSPF restart signaling.

Default Graceful restart

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# capability restart graceful
```

clear ip ospf process

Overview This command clears and restarts the OSPF routing process. Specify the Process ID to clear one particular OSPF process. When no Process ID is specified, this command clears all running OSPF processes.

Syntax

```
clear ip ospf [<0-65535>] process
```

Parameter	Description
<0-65535>	The Routing Process ID.

Mode Privileged Exec

Example

```
awplus# clear ip ospf process
```

compatible rfc1583

Overview This command changes the method used to calculate summary route to the that specified in RFC 1583. By default, OSPF uses the method specified in RFC 2328.

RFC 1583 specifies a method for calculating the metric for summary routes based on the minimum metric of the component paths available. RFC 2328 specifies a method for calculating metrics based on maximum cost.

It is possible that some ABRs in an area might conform to RFC 1583 and others support RFC 2328, which could lead to incompatibility in their interoperation. This command addresses this issue by allowing you to selectively disable compatibility with RFC 2328.

Use the **no** variant of this command to disable RFC 1583 compatibility.

Syntax

```
compatible rfc1583
no compatible rfc1583
```

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# compatible rfc1583
```

debug ospf events

Overview This command enables OSPF debugging for OSPF event troubleshooting.

To enable all debugging options, specify **debug ospf event** with no additional parameters.

The **no** and **undebug** variant of this command disable OSPF debugging. Use this command without parameters to disable all the options.

Syntax

```
debug ospf events [abr] [asbr] [lsa] [nssa] [os] [router]
[vlink]
```

```
no debug ospf events [abr] [asbr] [lsa] [nssa] [os] [router]
[vlink]
```

Parameter	Description
`abr`	Shows ABR events.
`asbr`	Shows ASBR events.
`lsa`	Shows LSA events.
`nssa`	Shows NSSA events.
`os`	Shows OS interaction events.
`router`	Shows other router events.
`vlink`	Shows virtual link events.

Mode Privileged Exec and Global Configuration

Example

```
awplus# debug ospf events asbr lsa
```

Related commands terminal monitor

undebug ospf events

debug ospf ifsm

Overview This command specifies debugging options for OSPF Interface Finite State Machine (IFSM) troubleshooting.

To enable all debugging options, specify **debug ospf ifsm** with no additional parameters.

The **no** and **undebug** variant of this command disable OSPF IFSM debugging. Use this command without parameters to disable all the options.

Syntax

```
debug ospf ifsm [status] [events] [timers]
no debug ospf ifsm [status] [events] [timers]
```

Parameter	Description
`events`	Displays IFSM event information.
`status`	Displays IFSM status information.
`timers`	Displays IFSM timer information.

Mode Privileged Exec and Global Configuration

Example

```
awplus# no debug ospf ifsm events status
awplus# debug ospf ifsm status
awplus# debug ospf ifsm timers
```

Related commands terminal monitor

undebug ospf ifsm

debug ospf lsa

Overview This command enables debugging options for OSPF Link State Advertisements (LSA) troubleshooting. This displays information related to internal operations of LSAs.

To enable all debugging options, specify **debug ospf lsa** with no additional parameters.

The **no** and **undebug** variant of this command disable OSPF LSA debugging. Use this command without parameters to disable all the options.

Syntax

```
debug ospf lsa [flooding] [generate] [install] [maxage]
[refresh]
```

```
no debug ospf lsa [flooding] [generate] [install] [maxage]
[refresh]
```

Parameter	Description
`flooding`	Displays LSA flooding.
`generate`	Displays LSA generation.
`install`	Show LSA installation.
`maxage`	Shows maximum age of the LSA in seconds.
`refresh`	Displays LSA refresh.

Mode Privileged Exec and Global Configuration

Examples

```
awplus# undebug ospf lsa refresh
```

Output Figure 28-1: Example output from the **debug ospf lsa** command

```
2002/05/09 14:08:11 OSPF: LSA[10.10.10.10:10.10.10.70]: instance(0x8139cd0)
created with Link State Update
2002/05/09 14:08:11 OSPF: RECV[LS-Upd]: From 10.10.10.70 via vlan5:10.10.10.50
(10.10.10.10 -> 224.0.0.5)
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: Begin send queue
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: # of LSAs 1, destination 224.0.0.5
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: End send queue
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: To 224.0.0.5 via vlan5:10.10.10.50
```

Related commands terminal monitor

undebug ospf lsa

debug ospf nfsm

Overview This command enables debugging options for OSPF Neighbor Finite State Machines (NFSMs).

To enable all debugging options, specify **debug ospf nfsm** with no additional parameters.

The **no** and **undebug** variant of this command disable OSPF NFSM debugging. Use this command without parameters to disable all the options.

Syntax

```
debug ospf nfsm [events] [status] [timers]
no debug ospf nfsm [events] [status] [timers]
```

Parameter	Description
`events`	Displays NFSM event information.
`status`	Displays NSFM status information.
`timers`	Displays NFSM timer information.

Mode Privileged Exec and Global Configuration

Examples

```
awplus# debug ospf nfsm events
awplus# no debug ospf nfsm timers
awplus# undebug ospf nfsm events
```

Related commands terminal monitor

undebug ospf nfsm

debug ospf nsm

Overview This command enables debugging options for the OSPF Network Service Module.

To enable both debugging options, specify **debug ospf nsm** with no additional parameters.

The **no** and **undebug** variant of this command disable OSPF NSM debugging. Use this command without parameters to disable both options.

Syntax

```
debug ospf nsm [interface] [redistribute]
no debug ospf nsm [interface] [redistribute]
```

Parameter	Description
`interface`	Specify NSM interface information.
`redistribute`	Specify NSM redistribute information.

Mode Priviledged Exec and Global Configuration

Examples

```
awplus# debug ospf nsm interface
awplus# no debug ospf nsm redistribute
awplus# undebug ospf nsm interface
```

Related commands terminal monitor

undebug ospf nsm

debug ospf packet

Overview This command enables debugging options for OSPF packets.

To enable all debugging options, specify **debug ospf packet** with no additional parameters.

The **no** and **undebug** variant of this command disable OSPF packet debugging. Use this command without parameters to disable all options.

Syntax

```
debug ospf packet [dd] [detail] [hello] [ls-ack] [ls-request]
[ls-update] [recv] [send]
```

```
no debug ospf packet [dd] [detail] [hello] [ls-ack] [ls-request]
[ls-update] [recv] [send]
```

Parameter	Description
`dd`	Specifies debugging for OSPF database descriptions.
`detail`	Sets the debug option to detailed information.
`hello`	Specifies debugging for OSPF hello packets.
`ls-ack`	Specifies debugging for OSPF link state acknowledgments.
`ls-request`	Specifies debugging for OSPF link state requests.
`ls-update`	Specifies debugging for OSPF link state updates.
`recv`	Specifies the debug option set for received packets.
`send`	Specifies the debug option set for sent packets.

Mode Privileged Exec and Global Configuration

Examples

```
awplus# debug ospf packet detail
awplus# debug ospf packet dd send detail
awplus# no debug ospf packet ls-request recv detail
awplus# undebug ospf packet ls-request recv detail
```

Related commands terminal monitor

undebug ospf packet

debug ospf route

Overview This command enables debugging of route calculation. Use this command without parameters to turn on all the options.

To enable all debugging options, specify **debug ospf route** with no additional parameters.

The **no** and **undebug** variant of this command disable OSPF route debugging. Use this command without parameters to disable all options.

Syntax

```
debug ospf route [ase] [ia] [install] [spf]
no debug ospf route [ase] [ia] [install] [spf]
```

Parameter	Description
`ia`	Specifies the debugging of Inter-Area route calculation.
`ase`	Specifies the debugging of external route calculation.
`install`	Specifies the debugging of route installation.
`spf`	Specifies the debugging of SPF calculation.

Mode Privileged Exec and Global Configuration

Examples

```
awplus# debug ospf route
awplus# no debug ospf route ia
awplus# debug ospf route install
awplus# undebug ospf route install
```

Related commands terminal monitor

undebug ospf route

default-information originate

Overview This command creates a default external route into an OSPF routing domain.

When you use the **default-information originate** command to redistribute routes into an OSPF routing domain, then the system acts like an Autonomous System Boundary Router (ASBR). By default, an ASBR does not generate a default route into the OSPF routing domain.

When using this command, also specify the **route-map** <*route-map*> option to avoid a dependency on the default network in the routing table.

The **metric-type** is an external link type associated with the default route advertised into the OSPF routing domain. The value of the external route could be either Type 1 or 2. The default is Type 2.

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

Syntax

```
default-information originate [always] [metric <metric>]
[metric-type <1-2>] [route-map <route-map>]
```

```
no default-information originate [always] [metric]
[metric-type] [route-map]
```

Parameter	Description
`always`	Used to advertise the default route regardless of whether there is a default route.
<metric>	The metric value used in creating the default route. Enter a value in the range 0 to 16777214. The default metric value is 10. The value used is specific to the protocol.
<1-2>	External metric type for default routes, either OSPF External Type 1 or Type 2 metrics. Enter the value 1 or 2.
`route-map`	Specifies to use a specific route-map.
<route-map>	The route-map name. It is a string comprised of any characters, numbers or symbols.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# default-information originate always
metric 23 metric-type 2 route-map myinfo
```

Related commands route-map

default-metric (OSPF)

Overview This command sets default metric values for the OSPF routing protocol.

The **no** variant of this command returns OSPF to using built-in, automatic metric translations, as appropriate for each routing protocol.

Syntax

```
default-metric <1-16777214>
no default-metric [<1-16777214>]
```

Parameter	Description
<1-16777214>	Default metric value appropriate for the specified routing protocol.

Mode Router Configuration

Usage notes A default metric facilitates redistributing routes even with incompatible metrics. If the metrics do not convert, the default metric provides an alternative and enables the redistribution to continue. The effect of this command is that OSPF will use the same metric value for **all** redistributed routes. Use this command in conjunction with the redistribute (OSPF) command.

Examples

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# default-metric 100
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# no default-metric
```

Related commands redistribute (OSPF)

distance (OSPF)

Overview This command sets the administrative distance for OSPF routes based on the route type. Your device uses this value to select between two or more routes to the same destination from two different routing protocols. The route with the smallest administrative distance value is added to the Forwarding Information Base (FIB). See the Route_Selection Feature Overview and Configuration Guide for more information.

Use the command **distance ospf** to set the distance for an entire category of OSPF routes, rather than the specific routes that pass an access list.

Use the command **distance <1-255>**, with no other parameter, to set the same distance for all OSPF route types.

The **no** variant of this command sets the administrative distance for all OSPF routes to the default of 110.

Syntax

```
distance <1-255>
distance ospf {external <1-255>|inter-area <1-255>|intra-area <1-255>}
no distance {ospf|<1-255>}
```

Parameter	Description
<1-255>	Specify the Administrative Distance value for OSPF routes.
`external`	Sets the distance for routes from other routing domains, learned by redistribution. Specify an OSPF external distance in the range *<1-255>*.
`inter-area`	Sets the distance for all routes from one area to another area. Specify an OSPF inter-area distance in the range *<1-255>*.
`intra-area`	Sets the distance for all routes within an area. Specify an OSPF intra-area distance in the range *<1-255>*.

Default The default OSPF administrative distance is 110. The default Administrative Distance for each type of route (intra, inter, or external) is 110.

Mode Router Configuration

Usage notes The administrative distance rates the trustworthiness of a routing information source. The distance could be any integer from 0 to 255. A higher distance value indicates a lower trust rating. For example, an administrative distance of 255 indicates that the routing information source cannot be trusted and should be ignored.

Use this command to set the distance for an entire group of routes, rather than a specific route that passes an access list.

Examples To set the following administrative distances for route types in OSPF 100:

- 20 for inter-area routes

- 10 for intra-area routes
- 40 for external routes

use the commands:

```
awplus(config)# router ospf 100
awplus(config-router)# distance ospf inter-area 20 intra-area
10 external 40
```

To set the administrative distance for all routes in OSPF 100 back to the default of 110, use the commands:

```
awplus(config)# router ospf 100
awplus(config-router)# no distance ospf
```

distribute-list (OSPF)

Overview Use this command to apply filtering to the transfer of routing information between OSPF and the IP route table. You can apply filtering in either direction, from OSPF to the IP route table using an **in** distribute-list or from the IP route table to OSPF using an **out** distribute-list.

The effect of an **in** filter is that some route information that OSPF has learned from LSA updates will not be installed into the IP route table. The effect of an **out** filter is that some route information that could be redistributed to OSPF will not be redistributed to OSPF. See the **Usage** section below for the distinction between the **in** and **out** distribute-lists.

The entities that are used to perform filtering are ACLs or route-maps, which match on certain attributes in the routes that are being transferred.

For information about ACLs and route maps, see the ACL Feature Overview and Configuration Guide and the Routemaps Feature Overview and Configuration Guide.

The **no** variant of this command removes the configured distribute-list command entry.

Syntax

```
distribute-list {<access-list-name>|route-map
<route-map-name>} in
```

```
distribute-list <access-list-name> out
{bgp|connected|rip|static}
```

```
no distribute-list <access-list-name> in
```

```
no distribute-list <access-list-name> out
{bgp|connected|rip|static}
```

Parameter	Description
<access-list-name>	Specifies the name of the access list. The access list defines which networks are received and which are suppressed.
`in`	Indicates that this applies to incoming advertised routes.
`out`	Indicates that this applies to outgoing advertised routes.
<route-map-name>	The name of the route-map that the distribute-list applies. This defines which networks are installed in the IP route table and which networks are filtered from the IP route table.
`bgp`	Specify the redistribution of BGP routes.
`connected`	Specify the redistribution of connected routes.
`rip`	Specify the redistribution of RIP routes.
`static`	Specify the redistribution of static routes.

Mode Router Configuration

Usage notes

There are **in** and **out** distribute-lists, which carry out different route filtering activities:

- The **in** distribute list is applied to the process of installing OSPF routes into the IP route table. The SPF calculations generate a set of routes calculated from the LSA database. By default, all of these routes become OSPF's candidate routes for inclusion into the IP route table.
- An **in** distribute-list can be used to control whether or not certain routes generated by the SPF calculation are included into the set of candidates for inclusion into the IP route table. Those routes that match **deny** entries in the distribute-list will not be considered for inclusion into the IP route table.
- The **out** distribute-list applies the process of redistributing non-OSPF routes into OSPF. If OSPF redistribution is configured, and an **out** distribute-list is also configured, then routes that match deny entries in the distribute-list will not be redistributed into OSPF.

Examples

The following example shows the installation of OSPF routes into the IP route table with route map "mymap1" applied, which will process routes that have been tagged 100:

```
awplus# configure terminal
awplus(config)# route-map mymap1 permit 10
awplus(config-route-map)# match tag 100
awplus(config-route-map)# exit
awplus(config)# router ospf 100
awplus(config-router)# distribute-list route-map mymap1 in
```

Use the following commands to configure a route-map to specifically prevent OSPF from offering 192.168.1.0/24 as a candidate for inclusion into the IP route table:

```
awplus# configure terminal
awplus(config)# ip prefix-list 100 seq 5 permit 192.168.1.0/24
awplus(config)# route-map 100 deny 10
awplus(config-route-map)# match ip address prefix-list 100
awplus(config-route-map)# exit
awplus(config)# route-map 100 permit 20
awplus(config-router)# router ospf 1
awplus(config-router)# distribute-list route-map 100 in
```

The following example shows the distribution of BGP routing updates into OSPF, based on the access list "myacl1" that is defined to permit network 172.10.0.0:

```
awplus# configure terminal
awplus(config)# access-list standard myacl1 permit
172.10.0.0/16
awplus(config)# router ospf 100
awplus(config-router)# distribute-list myacl1 out bgp
awplus(config-router)# redistribute bgp
```

Related commands

match interface

redistribute (OSPF)

route-map

enable db-summary-opt

Overview This command enables OSPF database summary list optimization.

The **no** variant of this command disables database summary list optimization.

Syntax

```
enable db-summary-opt
no enable db-summary-opt
```

Default The default setting is disabled.

Mode Router Configuration

Usage When this feature is enabled, the database exchange process is optimized by removing the LSA from the database summary list for the neighbor, if the LSA instance in the database summary list is the same as, or less recent than, the listed LSA in the database description packet received from the neighbor.

Examples To enable OSPF database summary list optimization, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf
awplus(config-router)# enable db-summary-opt
```

To disable OSPF database summary list optimization, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf
awplus(config-router)# no enable db-summary-opt
```

Validation Commands show running-config

host area

Overview This command configures a stub host entry belonging to a particular area. You can use this command to advertise specific host routes in the router-LSA as stub link. Since stub host belongs to the specified router, specifying cost is optional.

The **no** variant of this command removes the host area configuration.

Syntax

```
host <ip-address> area <area-id> [cost <0-65535>]
no host <ip-address> area <area-id> [cost <0-65535>]
```

Parameter	Description
<ip-address>	The IPv4 address of the host, in dotted decimal notation.
<area-id>	The OSPF area ID of the transit area that configuring the stub host entry for. Use one of the following formats: • dotted decimal format, e.g. 0.0.1.2. • normal decimal format in the range <0-4294967295>, e.g. 258.
`cost <0-65535>`	The cost for the stub host entry.

Default By default, no host entry is configured.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# host 172.16.10.100 area 1
awplus(config-router)# host 172.16.10.101 area 2 cost 10
```

ip ospf authentication

Overview This command sets the authentication method used when sending and receiving OSPF packets on the current VLAN interface. The default is to use no authentication. If no authentication method is specified in this command, then plain text authentication will be used.

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

Syntax

```
ip ospf [<ip-address>] authentication [message-digest|null]
no ip ospf [<ip-address>] authentication
```

Parameter	Description
<ip-address>	The IP address of the interface.
`message-digest`	Use the message digest authentication.
`null`	Use no authentication. It overrides password or message-digest authentication of the interface.

Mode Interface Configuration for a VLAN interface.

Usage notes Use the ip ospf authentication command to specify a Simple Text password. Use the ip ospf message-digest-key command to specify MD5 password.

Example In this example, VLAN interface `vlan2` is configured to have no authentication. This will override any text or MD5 authentication configured on this interface.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf authentication null
```

Related commands

ip ospf authentication-key

area authentication

ip ospf message-digest-key

ip ospf authentication-key

Overview This command specifies an OSPF authentication password for the neighboring routers.

The **no** variant of this command removes the OSPF authentication password.

Syntax

```
ip ospf [<ip-address>] authentication-key <pswd-long>
no ip ospf [<ip-address>] authentication-key
```

Parameter	Description
<ip-address>	The IPv4 address of the interface, in dotted decimal notation.
<pswd-long>	Specifies the authentication password. The string by the end of line will be used.

Default By default, an authentication password is not specified.

Mode Interface Configuration for a VLAN interface.

Usage notes This command creates a password (key) that is inserted into the OSPF header when AlliedWare Plus™ software originates routing protocol packets. Assign a separate password to each network for different VLAN interfaces. All neighboring routers on the same network with the same password exchange OSPF routing data.

The key can be used only when authentication is enabled for an area. Use the **area authentication** command to enable authentication.

Simple password authentication allows a password to be configured for each area. Configure the routers in the same routing domain with the same password.

Example In the following example, an authentication key test is created on VLAN interface `vlan2` in area 0. Note that first authentication is enabled for area 0.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# network 10.10.10.0/24 area 0
awplus(config-router)# area 0 authentication
awplus(config-router)# exit
awplus(config)# interface vlan2
awplus(config-if)# ip ospf 3.3.3.3 authentication-key test
```

Related commands

area authentication

ip ospf authentication

ip ospf cost

Overview This command explicitly specifies the cost of the link-state metric in a router-LSA.

The **no** variant of this command resets the VLAN interface cost to the default.

Syntax

```
ip ospf [<ip-address>] cost <1-65535>
no ip ospf [<ip-address>] cost
```

Parameter	Description
<ip-address>	The IPv4 address of the interface, in dotted decimal notation.
<1-65535>	The link-state metric.

Default By default there is no static value set and the OSPF cost is automatically calculated by using the auto-cost reference bandwidth command.

Mode Interface Configuration for a VLAN interface.

Usage notes This command explicitly sets a user specified cost of sending packets out the interface. Using this command overrides the cost value calculated automatically with the auto-cost reference bandwidth feature.

The interface cost indicates the overhead required to send packets across a certain VLAN interface. This cost is stated in the Router-LSA's link. Typically, the cost is inversely proportional to the bandwidth of an interface. By default, the cost of a VLAN interface is calculated according to the following formula:

reference bandwidth/interface bandwidth

To set the VLAN interface cost manually, use this command.

Example The following example shows setting ospf cost to 10 on VLAN interface `vlan25` for IP address 10.10.10.50

```
awplus# configure terminal
awplus(config)# interface vlan25
awplus(config-if)# ip ospf 10.10.10.50 cost 10
```

Related commands show ip ospf interface

auto-cost reference bandwidth

ip ospf database-filter

Overview This command turns on the LSA database-filter for a particular VLAN interface.

The **no** variant of this command turns off the LSA database-filter.

Syntax

```
ip ospf [<ip-address>] database-filter all out
no ip ospf [<ip-address>] database-filter
```

Parameter	Description
<ip-address>	The IPv4 address of the interface, in dotted decimal notation.

Default By default, all outgoing LSAs are flooded to the interface.

Mode Interface Configuration for a VLAN interface.

Usage notes OSPF floods new LSAs over all interfaces in an area, except the interface on which the LSA arrives. This redundancy ensures robust flooding. However, too much redundancy can waste bandwidth and might lead to excessive link and CPU usage in certain topologies, resulting in destabilizing the network. To avoid this, use the **ip ospf database-filter** command to block flooding of LSAs over specified interfaces.

Example

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if# ip ospf database-filter all out
```

ip ospf dead-interval

Overview This command sets the interval during which no hello packets are received and after which a neighbor is declared dead.

The dead-interval is the amount of time that OSPF waits to receive an OSPF hello packet from the neighbor before declaring the neighbor is down. This value is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

The **no** variant of this command returns the interval to the default of 40 seconds. If you have configured this command specifying the IP address of the interface and want to remove the configuration, specify the IP address (**no ip ospf**<*ip-address*> **dead-interval**).

Syntax

```
ip ospf [<ip-address>] dead-interval <1-65535>
no ip ospf [<ip-address>] dead-interval
```

Parameter	Description
<ip-address>	The IPv4 address of the interface, in dotted decimal notation.
<1-65545>	The interval in seconds. Default: 40

Mode Interface Configuration for a VLAN interface.

Example The following example shows configuring the dead-interval to 10 seconds on the VLAN interface `vlan2`.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf dead-interval 10
```

Related commands ip ospf hello-interval

show ip ospf interface

ip ospf disable all

Overview This command completely disables OSPF packet processing on a VLAN interface. It overrides the network area command and disables the processing of packets on the specific interface.

Use the **no** variant of this command to restore OSPF packet processing on a selected interface.

Syntax
```
ip ospf disable all
no ip ospf disable all
```

Mode Interface Configuration for a VLAN interface.

Example
```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf disable all
```

ip ospf hello-interval

Overview This command specifies the interval between hello packets.

The hello-interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter hello interval ensures faster detection of topological changes, but results in more routing traffic.

The **no** variant of this command returns the interval to the default of 10 seconds.

Syntax

```
ip ospf [<ip-address>] hello-interval <1-65535>
no ip ospf [<ip-address>] hello-interval
```

Parameter	Description
<ip-address>	The IP address of the interface, in dotted decimal notation.
<1-65535>	The interval in seconds. Default: 10

Default The default interval is 10 seconds.

Mode Interface Configuration for a VLAN interface.

Example The following example shows setting the hello-interval to 3 seconds on VLAN interface vlan2.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf hello-interval 3
```

Related commands

ip ospf dead-interval

show ip ospf interface

ip ospf message-digest-key

Overview This command registers an MD5 key for OSPF MD5 authentication.

Message Digest Authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a message digest that gets appended to the packet.

The **no** variant of this command removes the MD5 key.

Syntax

```
ip ospf [<ip-address>] message-digest-key <key-id> md5
<pswd-long>
```

```
no ip ospf [<ip-address>] message-digest-key <key-id>
```

Parameter	Description
<ip-address>	The IPv4 address of the interface, in dotted decimal notation.
<key-id>	A key ID number specified as an integer between 1 and 255.
`md5`	Use the MD5 algorithm.
<pswd-long>	The OSPF password. This is a string of 1 to 16 characters including spaces.

Default By default, there is no MD5 key registered.

Mode Interface Configuration for a VLAN interface.

Usage notes Use this command for uninterrupted transitions between passwords. It allows you to add a new key without having to delete the existing key. While multiple keys exist, all OSPF packets will be transmitted in duplicate; one copy of the packet will be transmitted for each of the current keys. This is helpful for administrators who want to change the OSPF password without disrupting communication. The system begins a rollover process until all the neighbors have adopted the new password. This allows neighboring routers to continue communication while the network administrator is updating them with a new password. The router will stop sending duplicate packets once it detects that all of its neighbors have adopted the new password.

Maintain only one password per interface, removing the old password whenever you add a new one. This will prevent the local system from continuing to communicate with the system that is using the old password. Removing the old password also reduces overhead during rollover. All neighboring routers on the same network must have the same password value to enable exchange of OSPF routing data.

Examples The following example shows OSPF authentication on the VLAN interface vlan5 when IP address has not been specified.

```
awplus# configure terminal
awplus(config)# interface vlan5
awplus(config-if)# ip ospf authentication message-digest
awplus(config-if)# ip ospf message-digest-key 1 md5 yourpass
```

The following example shows configuring OSPF authentication on the VLAN interface vlan2 for the IP address 1.1.1.1. (If the interface has two IP addresses assigned-- 1.1.1.1 & 2.2.2.2, OSPF authentication will be enabled only for the IP address 1.1.1.1).

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf 1.1.1.1 authentication
message-digest
awplus(config-if)# ip ospf 1.1.1.1 message-digest-key 2 md5
yourpass
```

ip ospf mtu

Overview This command sets the MTU size for OSPF. Whenever OSPF constructs packets, it uses the interface MTU size as Maximum IP packet size. This command forces OSPF to use the specified value, instead of the actual interface MTU size.

Use the **no** variant of this command to return the MTU size to the default.

Syntax

```
ip ospf mtu <576-65535>
no ip ospf mtu
```

Default By default, OSPF uses interface MTU derived from the interface.

Mode Interface Configuration for a VLAN interface.

Usage notes This command allows an administrator to configure the MTU size recognized by the OSPF protocol. It does not configure the MTU settings on the interface.

This command can be useful to ensure the OSPF neighbor relationship can fully establish via a network link, where the neighboring devices may have mismatched interface MTUs.

Example To change the OSPF MTU to 1446 on VLAN2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf mtu 1446
```

ip ospf mtu-ignore

Overview Use this command to configure OSPF so that OSPF does not check the MTU size during DD (Database Description) exchange.

Use the **no** variant of this command to make sure that OSPF checks the MTU size during DD exchange.

Syntax

```
ip ospf [<ip-address>] mtu-ignore
no ip ospf [<ip-address>] mtu-ignore
```

Parameter	Description
<ip-address>	IPv4 address of the interface, in dotted decimal notation.

Mode Interface Configuration for a VLAN interface.

Usage notes By default, during the DD exchange process, OSPF checks the MTU size described in the DD packets received from the neighbor. If the MTU size does not match the interface MTU, the neighbor adjacency is not established. Using this command makes OSPF ignore this check and allows establishing of adjacency regardless of MTU size in the DD packet.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf mtu-ignore
```

ip ospf network

Overview This command configures the OSPF network type to a type different from the default for the particular VLAN interface.

The **no** variant of this command returns the network type to the default for the particular VLAN interface.

Syntax

```
ip ospf network [broadcast|non-broadcast|point-to-point|
point-to-multipoint]
```

```
no ip ospf network
```

Parameter	Description
`broadcast`	Sets the network type to broadcast.
`non-broadcast`	Sets the network type to NBMA.
`point-to-multipoint`	Sets the network type to point-to-multipoint.
`point-to-point`	Sets the network type to point-to-point.

Default The default is the `broadcast` OSPF network type for a VLAN interface.

Mode Interface Configuration for a VLAN interface.

Usage notes This command forces the interface network type to the specified type. Depending on the network type, OSPF changes the behavior of the packet transmission and the link description in LSAs.

Example The following example shows setting the network type to point-to-point on the VLAN interface vlan2.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf network point-to-point
```

ip ospf priority

Overview This command sets the router priority, which is a parameter used in the election of the designated router for the network.

The **no** variant of this command returns the router priority to the default of 1.

Syntax

```
ip ospf [<ip-address>] priority <priority>
no ip ospf [<ip-address>] priority
```

Parameter	Description
<ip-address>	The IP address of the interface.
<priority>	*<0-255>* Specifies the Router Priority of the interface.

Default The router priority for an interface is set to 1 by default.

Mode Interface Configuration for a VLAN interface.

Usage notes Set the priority to help determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority becomes the DR. If the router priority is the same for two routers, the router with the higher router ID takes precedence.

Only routers with nonzero router priority values are eligible to become the designated or backup designated router.

Configure router priority for multi-access networks only and not for point-to-point networks.

Example The following example shows setting the OSPF priority value to 3 on the VLAN interface `vlan2`.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf priority 3
```

Related commands ip ospf network

ip ospf resync-timeout

Overview Use this command to set the interval after which adjacency is reset if out-of-band resynchronization has not occurred. The interval period starts from the time a restart signal is received from a neighbor.

Use the **no** variant of this command to return to the default.

Syntax

```
ip ospf [<ip-address>] resync-timeout <1-65535>
no ip ospf [<ip-address>] resync-timeout
```

Parameter	Description
<ip-address>	The IP address of the interface.
<1-65535>	Specifies the resynchronization timeout value of the interface in seconds.

Mode Interface Configuration for a VLAN interface.

Example The following example shows setting the OSPF resynchronization timeout value to 65 seconds on the VLAN interface `vlan2`.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf resync-timeout 65
```

ip ospf retransmit-interval

Overview Use this command to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.

Use the **no** variant of this command to return to the default of 5 seconds.

Syntax

```
ip ospf [<ip-address>] retransmit-interval <1-65535>
no ip ospf [<ip-address>] retransmit-interval
```

Parameter	Description
<ip-address>	The IP address of the interface.
<1-65535>	Specifies the interval in seconds.

Default The default interval is 5 seconds.

Mode Interface Configuration for a VLAN interface.

Usage notes After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgment. In case the router does not receive an acknowledgment during the set time (the retransmit interval value) it retransmits the LSA. Set the retransmission interval value conservatively to avoid needless retransmission. The interval should be greater than the expected round-trip delay between two routers.

Example The following example shows setting the `ospf retransmit interval` to 6 seconds on the VLAN interface `vlan2`.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf retransmit-interval 6
```

ip ospf transmit-delay

Overview Use this command to set the estimated time it takes to transmit a link-state-update packet on the VLAN interface.

Use the **no** variant of this command to return to the default of 1 second.

Syntax

```
ip ospf [<ip-address>] transmit-delay <1-65535>
no ip ospf [<ip-address>] transmit-delay
```

Parameter	Description
<ip-address>	The IP address of the VLAN interface.
<1-65535>	Specifies the time, in seconds, to transmit a link-state update.

Default The default interval is 1 second.

Mode Interface Configuration for a VLAN interface.

Usage notes The transmit delay value adds a specified time to the age field of an update. If the delay is not added, the time in which the LSA transmits over the link is not considered. This command is especially useful for low speed links. Add transmission and propagation delays when setting the transmit delay value.

Example The following example shows setting the OSPF transmit delay time to 3 seconds on the VLAN interface `vlan2`.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf transmit-delay 3
```

max-concurrent-dd

Overview Use this command to set the limit for the number of Database Descriptors (DD) that can be processed concurrently.

Use the **no** variant of this command to reset the limit for the number of Database Descriptors (DD) that can be processed concurrently.

Syntax

```
max-concurrent-dd <1-65535>
no max-concurrent-dd
```

Parameter	Description
<1-65535>	Specify the number of DD processes.

Mode Router Configuration

Usage This command is useful when a router's performance is affected from simultaneously bringing up several OSPF adjacencies. This command limits the maximum number of DD exchanges that can occur concurrently per OSPF instance, thus allowing for all of the adjacencies to come up.

Example The following example sets the max-concurrent-dd value to 4, so that only 4 DD exchanges will be processed at a time.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router# max-concurrent-dd 4
```

maximum-area

Overview Use this command to set the maximum number of OSPF areas.

Use the **no** variant of this command to set the maximum number of OSPF areas to the default.

Syntax

```
maximum-area <1-4294967294>
no maximum-area
```

Parameter	Description
<1-4294967294>	Specify the maximum number of OSPF areas.

Default The default for the maximum number of OSPF areas is 4294967294.

Mode Router Configuration

Usage notes Use this command in router OSPF mode to specify the maximum number of OSPF areas.

Examples The following example sets the maximum number of OSPF areas to 2:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# maximum-area 2
```

The following example removes the maximum number of OSPF areas and resets to default:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# no maximum-area
```

neighbor (OSPF)

Overview Use this command to inform the router of other neighboring routers that are connected to the same NBMA network.

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

Syntax

```
neighbor <ip-address> [<cost>]{<priority>|<poll-interval>}
no neighbor <ip-address> [<cost>]{<priority>|<poll-interval>}
```

Parameter	Description
<ip-address>	Specifies the interface IP address of the neighbor.
<priority>	*priority <0-255>* Specifies the router priority value of the non-broadcast neighbor associated with the specified IP address. The default is 0. This keyword does not apply to point-to-multipoint interfaces.
<poll-interval>	*poll-interval <1-2147483647>* Dead neighbor polling interval in seconds. It is recommended to set this value much higher than the hello interval. The default is 120 seconds.
<cost>	*cost <1-65535>* Specifies the link-state metric to this neighbor.

Mode Router Configuration

Usage To configure a neighbor on an NBMA network manually, use the `neighbor` command and include one neighbor entry for each known nonbroadcast network neighbor. The IP address used in this command is the neighbor's primary IP address on the interface where that neighbor connects to the NBMA network.

The poll interval is the reduced rate at which routers continue to send hello packets, when a neighboring router has become inactive. Set the poll interval to be much larger than hello interval.

Examples This example shows a neighbor configured with a priority value, poll interval time, and cost.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# neighbor 1.2.3.4 priority 1
poll-interval 90
awplus(config-router)# neighbor 1.2.3.4 cost 15
```

network area

Overview Use this command to enable OSPF routing with a specified Area ID on any interfaces with IP addresses that match the specified network address.

Use the **no** variant of this command to disable OSPF routing on the interfaces.

Syntax

```
network <network-address> area <area-id>
no network <network-address> area <area-id>
```

Parameter		Description
<network-address>		*{<ip-network/m>|<ip-addr> <reverse-mask>}*
	<ip-network/m>	IP address of the network, entered in the form A.B.C.D/M. Dotted decimal notation followed by a forward slash, and then the subnet mask length.
	<ip-addr> <reverse-mask>	IPv4 network address, entered in the form A.B.C.D, followed by the mask. Enter the mask as a wildcard, or reverse, mask (e.g. 0.0.0.255). Note that the device displays the mask as a subnet mask in the running configuration.
<area-id>		*{<ip-addr>|<0-4294967295>}*
	<ip-addr>	OSPF Area ID in IPv4 address format, in the form A.B.C.D.
	<0-4294967295>	OSPF Area ID as 4 octets unsigned integer value.

Default No **network area** is configured by default.

Mode Router Configuration

Usage notes OSPF routing can be enabled per IPv4 subnet. The network address can be defined using either the prefix length or a wild card mask. A wild card mask is comprised of consecutive `0's` as network bits and consecutive `1's` as host bits.

Examples The following commands show the use of the **network area** command with OSPF multiple instance support disabled:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# network 10.0.0.0/8 area 3
awplus(config-router)# network 10.0.0.0/8 area 1.1.1.1
```

The following commands disable OSPF routing with Area ID 3 on all interfaces:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# no network 10.0.0.0/8 area3
```

ospf abr-type

Overview Use this command to set an OSPF Area Border Router (ABR) type.

Use the **no** variant of this command to revert the ABR type to the default setting (Cisco).

Syntax

```
ospf abr-type {cisco|ibm|standard}
no ospf abr-type {cisco|ibm|standard}
```

Parameter	Description
`cisco`	Specifies an alternative ABR using Cisco implementation (RFC 3509). This is the default ABR type.
`ibm`	Specifies an alternative ABR using IBM implementation (RFC 3509).
`standard`	Specifies a standard behavior ABR (RFC 2328).

Default ABR type `Cisco`

Mode Router Configuration

Usage Specifying the ABR type allows better interoperation between different implementations. This command is specially useful in a multi-vendor environment. The different ABR types are:

- Cisco ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached and one of them is the backbone area.
- IBM ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached and the backbone area is configured. In this case the configured backbone need not be actively connected.
- Standard ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached to it.

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# ospf abr-type ibm
```

ospf restart grace-period

Overview Use this command to configure the grace-period for restarting OSPF routing.

Use the **no** variant of this command to revert to the default grace-period.

Syntax

```
ospf restart grace-period <1-1800>
no ospf restart grace-period
```

Parameter	Description
<1-1800>	Specifies the grace period in seconds.

Default In the AlliedWare Plus™ OSPF implementation, the default OSPF grace-period is 180 seconds.

Mode Global Configuration

Usage notes Use this command to enable the OSPF Graceful Restart feature and set the restart grace-period. Changes from the default restart grace-period are displayed in the running- config. The restart grace-period is not displayed in the running-config if it has been reset to the default using the **no** variant of this command.

Example To set the OSPF restart grace-period to 250 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ospf restart grace-period 250
```

To reset the OSPF restart grace-period to the default (180 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# no ospf restart grace-period
```

Validation Commands show running-config

Related commands ospf restart helper

restart ospf graceful

ospf restart helper

Overview Use this command to configure the **helper** behavior for the OSPF Graceful Restart feature.

Use the **no** variant of this command to revert to the default grace-period.

Syntax

```
ospf restart helper {max-grace-period <grace-period>|only-reload|only-upgrade}
ospf restart helper {never router-id <router-id>}
no ospf restart helper [max-grace-period]
```

Parameter	Description
`max-grace-period`	Specify help if received grace-period is less than a specified value.
<grace-period>	Maximum grace period accepted in seconds in range *<1-1800>*.
`never`	Specify the local policy to never to act as a helper for this feature.
`only-reload`	Specify help only on software reloads not software upgrades.
`only-upgrade`	Specify help only on software upgrades not software reloads.
`router-id`	Enter the router-id keyword to specify the OSPF Router ID that is never to act as a helper for the OSPF Graceful Restart feature.
<router-id>	*<A.B.C.D>* Specify the OSPF Router ID in dotted decimal format A.B.C.D

Default In the AlliedWare Plus™ OSPF implementation, the default OSPF grace-period is 180 seconds.

Mode Global Configuration

Usage The **ospf restart helper** command requires at least one parameter, but you may use more than one in the same command (excluding parameter **never**).

The **no** version of this command turns off the OSPF restart helper, while the **no ospf restart helper max-grace-period** command resets the max-grace-period, rather than the helper policy itself.

Example

```
awplus# configure terminal
awplus(config)# ospf restart helper only-reload
awplus# configure terminal
awplus(config)# ospf restart helper never router-id 10.10.10.1
awplus# configure terminal
awplus(config)# no ospf restart helper max-grace-period
```

Related commands

ospf restart grace-period

restart ospf graceful

ospf router-id

Overview Use this command to specify a router ID for the OSPF process.

Use the **no** variant of this command to disable this function.

Syntax

```
ospf router-id <ip-address>
no ospf router-id
```

Parameter	Description
<ip-address>	Specifies the router ID in IPv4 address format.

Mode Router Configuration

Usage Configure each router with a unique router-id. In an OSPF router process that has active neighbors, a new router-id takes effect at the next reload or when you restart OSPF manually.

Example The following example shows a specified router ID 2.3.4.5.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# ospf router-id 2.3.4.5
```

Related commands show ip ospf

overflow database

Overview Use this command to limit the maximum number of Link State Advertisements (LSAs) that can be supported by the current OSPF instance.

Use the **no** variant of this command to have no limit on the maximum number of LSAs.

Syntax

```
overflow database <0-4294967294> {hard|soft}
no overflow database
```

Parameter	Description
<0-4294967294>	The maximum number of LSAs.
`hard`	Shutdown occurs if the number of LSAs exceeds the specified value.
`soft`	Warning message appears if the number of LSAs exceeds the specified value.

Mode Router Configuration

Usage Use **hard** with this command if a shutdown is required if the number of LSAs exceeds the specified number. Use **soft** with this command if a shutdown is not required, but a warning message is required, if the number of LSAs exceeds the specified number.

Example The following example shows setting the database overflow to 500, and a shutdown to occur, if the number of LSAs exceeds 500.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# overflow database 500 hard
```

overflow database external

Overview Use this command to configure the size of the external database and the time the router waits before it tries to exit the overflow state.

Use the **no** variant of this command to revert to default.

Syntax

```
overflow database external <max-lsas> <recover-time>
no overflow database external
```

Parameter	Description
<max-lsas>	*<0-2147483647>* The maximum number of Link State Advertisements (LSAs). Note that this value should be the same on all routers in the AS.
<recover-time>	*<0-65535>* the number of seconds the router waits before trying to exit the database overflow state. If this parameter is 0, router exits the overflow state only after an explicit administrator command.

Mode Router Configuration

Usage Use this command to limit the number of AS-external-LSAs a router can receive, once it is in the wait state. It takes the number of seconds specified as the *<recover-time>* to recover from this state.

Example The following example shows setting the maximum number of LSAs to 5 and the time to recover from overflow state to be 3:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# overflow database external 50 3
```

passive-interface (OSPF)

Overview Use this command to suppress the sending of Hello packets on all interfaces, or on a specified interface. If you use the **passive-interface** command without the optional parameters then **all** interfaces are put into passive mode.

Use the **no** variant of this command to allow the sending of Hello packets on all interfaces, or on the specified interface. If you use the **no** variant of this command without the optional parameters then **all** interfaces are removed from passive mode.

Syntax

```
passive-interface [<interface>][<ip-address>]
no passive-interface [<interface>][<ip-address>]
```

Parameter	Description
<interface>	The name of the interface.
<ip-address>	IP address of the interface, entered in the form A.B.C.D.

Mode Router Configuration

Usage notes Configure an interface to be passive if you wish its connected route to be treated as an OSPF route (rather than an AS-external route), but do not wish to actually exchange any OSPF packets via this interface.

Examples To configure passive interface mode on **all** interfaces, enter the following commands:

```
awplus(config)# router ospf 100
awplus(config-router)# passive-interface
```

To remove passive interface mode on interface vlan2, enter the following commands:

```
awplus(config)# router ospf 100
awplus(config-router)# no passive-interface vlan2
```

To remove passive interface mode on **all** interfaces, enter the following commands:

```
awplus(config)# router ospf 100
awplus(config-router)# no passive-interface
```

redistribute (OSPF)

Overview Use this command to redistribute routes from other routing protocols, static routes and connected routes into an OSPF routing table.

Use the **no** variant of this command to disable this function.

Syntax

```
redistribute {bgp|connected|rip|static} {metric
<0-16777214>|metric-type {1|2}|route-map <name>|tag
<0-4294967295>}
```

```
no redistribute {bgp|connected|rip|static} {metric
<0-16777214>|metric-type {1|2}|route-map <name>|tag
<0-4294967295>}
```

Parameter	Description
`bgp`	Specifies that this applies to the redistribution of BGP routes.
`connected`	Specifies that this applies to the redistribution of connected routes.
`rip`	Specifies that this applies to the redistribution of RIP routes.
`static`	Specifies that this applies to the redistribution of static routes.
`metric`	Specifies the external metric.
`metric-type`	Specifies the external metric-type.
`route-map`	Specifies name of the route-map.
`tag`	Specifies the external route tag.

Default The default metric value for routes redistributed into OSPF is 20. The metric can also be defined using the set metric command for a route map. Note that a metric defined using the set metric command for a route map overrides a metric defined with this command.

Mode Router Configuration

Usage notes You use this command to inject routes, learned from other routing protocols, into the OSPF domain to generate AS-external-LSAs. If a route-map is configured by this command, then that route-map is used to control which routes are redistributed and can set metric and tag values on particular routes.

The metric, metric-type, and tag values specified on this command are applied to any redistributed routes that are not explicitly given a different metric, metric-type, or tag value by the route map.

See the OSPF Feature Overview and Configuration Guide for more information about metrics, and about behavior when configured in route maps.

Note that this command does not redistribute the default route. To redistribute the default route, use the default-information originate command.

Example The following example shows redistribution of BGP routes into OSPF routing table 100, with metric 12.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# redistribute bgp metric 12
```

The following example shows the configuration of a route-map named `rmap2`, which is then applied using the **redistribute route-map** command, so routes learned via interface vlan1 can be redistributed as type-1 external LSAs:

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 3
awplus(config-route-map)# match interface vlan1
awplus(config-route-map)# set metric-type 1
awplus(config-route-map)# exit
awplus(config)# router ospf 100
awplus(config-router)# redistribute rip route-map rmap2
```

Note that configuring a route-map and applying it with the **redistribute route-map** command allows you to filter which routes are distributed from another routing protocol (such as RIP). A route-map can also set the metric, tag, and metric-type of the redistributed routes.

Related commands

distribute-list (OSPF)

match interface

route-map

show ip ospf database external

restart ospf graceful

Overview Use this command to force the OSPF process to restart, and optionally set the grace-period.

Syntax

```
restart ospf graceful [grace-period <1-1800>]
```

Parameter	Description
`grace-period`	Specify the grace period.
<1-1800>	The grace period in seconds.

Default In the AlliedWare Plus™ OSPF implementation, the default OSPF grace-period is 180 seconds.

Mode Privileged Exec

Usage notes After this command is executed, the OSPF process immediately shuts down. It notifies the system that OSPF has performed a graceful shutdown. Routes installed by OSPF are preserved until the grace-period expires.

When a **restart ospf graceful** command is issued, the OSPF configuration is reloaded from the last saved configuration. Ensure you first enter the command copy running-config startup-config.

Example

```
awplus# copy running-config startup-config
awplus# restart ospf graceful grace-period 200
```

Related commands ospf restart grace-period

ospf restart helper

router ospf

Overview Use this command to enter Router Configuration mode to configure an OSPF routing process. You must specify the process ID with this command for multiple OSPF routing processes on the device.

Use the **no** variant of this command to terminate an OSPF routing process.

Use the **no** parameter with the **process-id** parameter, to terminate and delete a specific OSPF routing process. If no **process-id** is specified on the **no** variant of this command, then all OSPF routing processes are terminated, and all OSPF configuration is removed.

Syntax

```
router ospf [<process-id>]
no router ospf [<process-id>]
```

Parameter	Description
<process-id>	A positive number from 1 to 65535, that is used to define a routing process.

Default No routing process is defined by default.

Mode Global Configuration

Usage notes The process ID of OSPF is an optional parameter for the **no** variant of this command only. When removing all instances of OSPF, you do not need to specify each Process ID, but when removing particular instances of OSPF you must specify each Process ID to be removed.

Example To enter Router Configuration mode to configure an existing OSPF routing process `100`, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)#
```

router-id

Overview Use this command to specify a router ID for the OSPF process.

Use the **no** variant of this command to force OSPF to use the previous OSPF router-id behavior.

Syntax

```
router-id <ip-address>
no router-id
```

Parameter	Description
<ip-address>	Specifies the router ID in IPv4 address format.

Mode Router Configuration

Usage Configure each router with a unique router-id. In an OSPF router process that has active neighbors, a new router-id is used at the next reload or when you restart OSPF manually.

Example The following example shows a fixed router ID 10.10.10.60

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# router-id 10.10.10.60
```

Related commands show ip ospf

show debugging ospf

Overview Use this command to see what debugging is turned on for OSPF.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show debugging ospf
```

Mode User Exec and Privileged Exec

Example

```
awplus# show debugging ospf
```

Output Figure 28-2: Example output from the **show debugging ospf** command

```
OSPF debugging status:
  OSPF packet Link State Update debugging is on
  OSPF all events debugging is on
```

show ip ospf

Overview Use this command to display general information about all OSPF routing processes. Include the process ID parameter with this command to display information about specified instances.

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

Syntax

```
show ip ospf
show ip ospf <process-id>
```

Parameter	Description
<process-id>	*<0-65535>* The ID of the router process for which information will be displayed. If this parameter is included, only the information for the specified routing process is displayed.

Mode User Exec and Privileged Exec

Examples To display general information about all OSPF routing processes, use the command:

```
awplus# show ip ospf
```

To display general information about OSPF routing process `100`, use the command:

```
awplus# show ip ospf 100
```

Table 1: Example output from the **show ip ospf** command

```
Route Licence: Route : Limit=0, Allocated=0, Visible=0, Internal=0
Route Licence: Breach: Current=0, Watermark=0
Routing Process "ospf 10" with ID 192.168.1.1
Process uptime is 10 hours 24 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Graceful Restart
SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs
Refresh timer 10 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 0
```

Table 1: Example output from the **show ip ospf** command (cont.)

```
External LSA database is unlimited.
Number of LSA originated 0
Number of LSA received 0
Number of areas attached to this router: 2
   Area 0 (BACKBONE) (Inactive)
       Number of interfaces in this area is 0(0)
       Number of fully adjacent neighbors in this area is 0
       Area has no authentication
       SPF algorithm executed 0 times
       Number of LSA 0. Checksum 0x000000

   Area 1 (Inactive)
       Number of interfaces in this area is 0(0)
       Number of fully adjacent neighbors in this area is 0
       Number of fully adjacent virtual neighbors through this area is 0
       Area has no authentication
       SPF algorithm executed 0 times
       Number of LSA 0. Checksum 0x000000
```

Table 2: Example output from the **show ip ospf <process-id>** command

```
Routing Process "ospf 100" with ID 10.10.11.146
Process uptime is 0 minute
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x0
Number of non-default external LSA 0
External LSA database is unlimited.
Number of areas attached to this router: 1
   Area 1
       Number of interfaces in this area is 1(1)
       Number of fully adjacent neighbors in this area is 0
       Number of fully adjacent virtual neighbors through this area is 0
       Area has no authentication
       SPF algorithm executed 0 times
       Number of LSA 1. Checksum Sum 0x00e3e2
```

Table 3: Parameters in the output of the **show ip ospf** command

Output Parameter		Meaning
`Route Licence: Route:`	`Limit`	The maximum number of OSPF routes which may be used for forwarding.
	`Allocated`	The current total number of OSPF routes allocated in the OSPF module.
	`Visible`	The current number of OSPF routes which may be used for forwarding.
	`Internal`	The number of OSPF internal routes used for calculating paths to ASBRs.
`Number of external LSA`		The number of external link-state advertisements
`Number of opaque AS LSA`		Number of opaque link-state advertisements

Related commands router ospf

show ip ospf border-routers

Overview Use this command to display the ABRs and ASBRs for all OSPF instances. Include the process ID parameter with this command to view data about specified instances.

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

Syntax

```
show ip ospf border-routers
show ip ospf <process-id> border-routers
```

Parameter	Description
<process-id>	*<0-65535>* The ID of the router process for which information will be displayed.

Mode User Exec and Privileged Exec

Output Figure 28-3: Example output from the **show ip ospf border-routers** command

```
OSPF process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.15.0.1 [10] via 10.10.0.1, vlan2, ASBR, Area 0.0.0.0
i 172.16.10.1 [10] via 10.10.11.50, vlan3, ABR, ASBR, Area
0.0.0.0
```

show ip ospf database

Overview Use this command to display a database summary for OSPF information. Include the process ID parameter with this command to display information about specified instances.

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

Syntax

```
show ip ospf [<process-id>] database
[self-originate|max-age|adv router <adv-router-id>]
```

Parameter	Description
<process-id>	*<0-65535>* The ID of the router process for which information will be displayed.
`self-originate`	Displays self-originated link states.
`max-age`	Displays LSAs in MaxAge list. It maintains the list of the all LSAs in the database which have reached the max-age which is 3600 seconds.
`adv-router`	Advertising Router LSA.
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.

Mode User Exec and Privileged Exec

Examples To display the ABRs and ASBRs for all OSPF instances, use the command:

```
awplus# show ip ospf border-routers
```

To display the ABRs and ASBRs for the specific OSPF instance `721`, use the command:

```
awplus# show ip ospf 721 border-routers
```

Output Figure 28-4: Example output from the **show ip ospf database** command

```
       OSPF Router process 1 with ID (10.10.11.60)
                Router Link States (Area 0.0.0.1)
Link ID         ADV Router      Age  Seq#       CkSum  Link
count
10.10.11.60     10.10.11.60       32 0x80000002 0x472b 1
       OSPF Router process 100 with ID (10.10.11.60)
                Router Link States (Area 0.0.0.0)
Link ID         ADV Router      Age  Seq#       CkSum  Link
count
10.10.11.60     10.10.11.60      219 0x80000001 0x4f5d 0
```

Example

```
awplus# show ip ospf database external 1.2.3.4 self-originate
awplus# show ip ospf database self-originate
```

Figure 28-5: Example output from the **show ip ospf database self-originate** command

```
       OSPF Router process 100 with ID (10.10.11.50)
                Router Link States (Area 0.0.0.1 [NSSA])
Link ID         ADV Router      Age  Seq#       CkSum  Link
count
10.10.11.50     10.10.11.50     20  0x80000007  0x65c3 2
                Area-Local Opaque-LSA (Area 0.0.0.1 [NSSA])
Link ID         ADV Router      Age  Seq#       CkSum Opaque ID
67.1.4.217      10.10.11.50     37 0x80000001  0x2129 66777
                AS-Global Opaque-LSA
Link ID         ADV Router      Age  Seq#       CkSum Opaque ID
67.1.4.217      10.10.11.50     37 0x80000001  0x2daa 66777
```

show ip ospf database asbr-summary

Overview Use this command to display information about the Autonomous System Boundary Router (ASBR) summary LSAs.

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

Syntax

```
show ip ospf database asbr-summary [<ip-addr>]
[self-originate|adv-router <advrouter-ip-addr>]
```

Parameter	Description
<ip-addr>	A link state ID, as an IP address.
`self-originate`	Displays self-originated link states.
adv-router <advrouter-ip-addr>	Displays all the LSAs of the specified router.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database asbr-summary 1.2.3.4
self-originate
```

```
awplus# show ip ospf database asbr-summary self-originate
```

```
awplus# show ip ospf database asbr-summary 1.2.3.4 adv-router
2.3.4.5
```

show ip ospf database external

Overview Use this command to display information about the external LSAs.

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

Syntax

```
show ip ospf database external adv-router[<adv-router-id>]
[self-originate|adv-router<adv-router-id>]
```

Parameter	Description
`adv-router`	Displays all the LSAs of the specified router.
`self-originate`	Displays self-originated link states.
<adv-router- id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database external 1.2.3.4 self-originate
awplus# show ip ospf database external self-originate
awplus# show ip ospf database external 1.2.3.4 adv-router
2.3.4.5
```

Output Figure 28-6: Example output from the **show ip ospf database external self-originate** command

```
      OSPF Router process 100 with ID (10.10.11.50)
                AS External Link States
  LS age: 298
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 10.10.100.0 (External Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x7033
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 10.10.11.50
        External Route Tag: 0
```

Output Figure 28-7: Example output from the **show ip ospf database external adv-router** command

```
awplus#show ip ospf database external adv-router 1.1.1.1

                 AS External Link States
LS age: 273
Options: 0x2 (-|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 1.1.1.1
LS Seq Number: 80000004
Checksum: 0x02f8
Length: 36
Network Mask: /24
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 20
      Forward Address: 0.0.0.0
      External Route Tag: 0
```

show ip ospf database network

Overview Use this command to display information about the network LSAs.

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

Syntax

```
show ip ospf database network [<adv-router-id>]
[self-originate|<adv-router-id>]
```

Parameter	Description
<adv-router-id>	The router ID of the advertising router, in IPv4 address format. Note however, that this no longer represents a real address.
`self-originate`	Displays self-originated link states.
`adv-router`	Displays all the LSAs of the specified router.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database network 1.2.3.4 self-originate
awplus# show ip ospf database network self-originate
awplus# show ip ospf database network 1.2.3.4 adv-router 2.3.4.5
```

Output Figure 28-8: Example output from the **show ip ospf database network** command

```
      OSPF Router process 200 with ID (192.30.30.2)
                Net Link States (Area 0.0.0.0)
  LS age: 1387
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
  Link State ID: 192.10.10.9 (address of Designated Router)
  Advertising Router: 192.30.30.3
  LS Seq Number: 80000001
  Checksum: 0xe1b0
  Length: 32
  Network Mask: /24
        Attached Router: 192.20.20.1
        Attached Router: 192.30.30.3
      OSPF Router process 200 with ID (192.30.30.2)
                Net Link States (Area 0.0.0.0)
...
```

show ip ospf database nssa-external

Overview Use this command to display information about the NSSA external LSAs.

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

Syntax

```
show ip ospf database nssa-external [<ip-address>]
[self-originate|<advrouter>]
```

Parameter	Description
<advrouter>	adv-router <ip-address>
adv-router	Displays all the LSAs of the specified router.
<ip-address>	A link state ID, as an IP address.
self-originate	Displays self-originated link states.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database nssa-external 1.2.3.4
self-originate
```

```
awplus# show ip ospf database nssa-external self-originate
```

```
awplus# show ip ospf database nssa-external 1.2.3.4 adv-router
2.3.4.5
```

Output Figure 28-9: Example output from the **show ip ospf database nssa-external adv-router** command

```
      OSPF Router process 100 with ID (10.10.11.50)
               NSSA-external Link States (Area 0.0.0.0)
               NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 78
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 0.0.0.0 (External Network Number For NSSA)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0xc9b6
Length: 36
Network Mask: /0
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 1
      NSSA: Forward Address: 0.0.0.0
```

```
        OSPF Router process 100 with ID (10.10.11.50)
                NSSA-external Link States (Area 0.0.0.0)
                NSSA-external Link States (Area 0.0.0.1 [NSSA])
  LS age: 78
  Options: 0x0 (*|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 0.0.0.0 (External Network Number For NSSA)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0xc9b6
  Length: 36
  Network Mask: /0
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 1
        NSSA: Forward Address: 0.0.0.0
        External Route Tag: 0
                 NSSA-external Link States (Area 0.0.0.1 [NSSA])
```

show ip ospf database opaque-area

Overview Use this command to display information about the area-local (link state type 10) scope LSAs. Type-10 Opaque LSAs are not flooded beyond the borders of their associated area.

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

Syntax

```
show ip ospf database opaque-area [<ip-address>]
[self-originate|<advrouter>]
```

Parameter	Description
<advrouter>	adv-router <ip-address>
adv-router	Displays all the LSAs of the specified router.
<ip-address>	A link state ID, as an IP address.
self-originate	Displays self-originated link states.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database opaque-area 1.2.3.4
self-originate
```

```
awplus# show ip ospf database opaque-area self-originate
```

```
awplus# show ip ospf database opaque-area 1.2.3.4 adv-router
2.3.4.5
```

Output Figure 28-10: Example output from the **show ip ospf database opaque-area** command

```
       OSPF Router process 100 with ID (10.10.11.50)
                Area-Local Opaque-LSA (Area 0.0.0.0)
  LS age: 262
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: Area-Local Opaque-LSA
  Link State ID: 10.0.25.176 (Area-Local Opaque-Type/ID)
  Opaque Type: 10
  Opaque ID: 6576
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0xb413
  Length: 26
```

show ip ospf database opaque-as

Overview Use this command to display information about the link-state type 11 LSAs. This type of link-state denotes that the LSA is flooded throughout the Autonomous System (AS).

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

Syntax

```
show ip ospf database opaque-as [<ip-address>]
[self-originate|<advrouter>]
```

Parameter	Description
<advrouter>	adv-router <ip-address>
adv-router	Displays all the LSAs of the specified router.
<ip-address>	A link state ID, as an IP address.
self-originate	Displays self-originated link states.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database opaque-as 1.2.3.4 self-originate
awplus# show ip ospf database opaque-as self-originate
awplus# show ip ospf database opaque-as 1.2.3.4 adv-router
2.3.4.5
```

Output Figure 28-11: Example output from the **show ip ospf database opaque-as** command

```
       OSPF Router process 100 with ID (10.10.11.50)
                AS-Global Opaque-LSA
  LS age: 325
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external Opaque-LSA
  Link State ID: 11.10.9.23 (AS-external Opaque-Type/ID)
  Opaque Type: 11
  Opaque ID: 657687
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0xb018
  Length: 25
```

show ip ospf database opaque-link

Overview Use this command to display information about the link-state type 9 LSAs. This type denotes a link-local scope. The LSAs are not flooded beyond the local network.

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

Syntax

```
show ip ospf database opaque-link [<ip-address>]
[self-originate|<advrouter>]
```

Parameter	Description
<advrouter>	adv-router <ip-address>
adv-router	Displays all the LSAs of the specified router.
<ip-address>	A link state ID, as an IP address.
self-originate	Displays self-originated link states.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database opaque-link 1.2.3.4
self-originate
```

```
awplus# show ip ospf database opaque-link self-originate
```

```
awplus# show ip ospf database opaque-link 1.2.3.4 adv-router
2.3.4.5
```

Output Figure 28-12: Example output from the **show ip ospf database opaque-link** command

```
       OSPF Router process 100 with ID (10.10.11.50)
                Link-Local Opaque-LSA (Link hme0:10.10.10.50)
  LS age: 276
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: Link-Local Opaque-LSA
  Link State ID: 10.0.220.247 (Link-Local Opaque-Type/ID)
  Opaque Type: 10
  Opaque ID: 56567
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x744e
  Length: 26
                Link-Local Opaque-LSA (Link hme1:10.10.11.50)
```

show ip ospf database router

Overview Use this command to display information only about the router LSAs.

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

Syntax

```
show ip ospf database router [<adv-router-id>
self-originate|<adv-router-id>]
```

Parameter	Description
`adv-router`	Displays all the LSAs of the specified router.
`self-originate`	Displays self-originated link states.
`<adv-router- id>`	The router ID of the advertising router, in IPv4 address format. Note however, that this no longer represents a real address.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database router 1.2.3.4 self-originate
awplus# show ip ospf database router self-originate
awplus# show ip ospf database router 1.2.3.4 adv-router 2.3.4.5
```

Output Figure 28-13: Example output from the **show ip ospf database router** command

```
       OSPF Router process 100 with ID (10.10.11.50)
                Router Link States (Area 0.0.0.0)
  LS age: 878
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.10.11.50
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000004
  Checksum: 0xe39e
  Length: 36
   Number of Links: 1
    Link connected to: Stub Network
     (Link ID) Network/subnet number: 10.10.10.0
     (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
       TOS 0 Metric: 10
```

```
               Router Link States (Area 0.0.0.1)
  LS age: 877
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.10.11.50
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000003
  Checksum: 0xee93
  Length: 36
   Number of Links: 1
    Link connected to: Stub Network
     (Link ID) Network/subnet number: 10.10.11.0
     (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
       TOS 0 Metric: 10
```

show ip ospf database summary

Overview Use this command to display information about the summary LSAs.

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

Syntax

```
show ip ospf database summary [<ip-address>]
[self-originate|<advrouter>]
```

Parameter	Description
<advrouter>	adv-router <ip-address>
adv-router	Displays all the LSAs of the specified router.
<ip-address>	A link state ID, as an IP address.
self-originate	Displays self-originated link states.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database summary 1.2.3.4 self-originate
awplus# show ip ospf database summary self-originate
awplus# show ip ospf database summary 1.2.3.4 adv-router 2.3.4.5
```

Output Figure 28-14: Example output from the **show ip ospf database summary** command

```
       OSPF Router process 100 with ID (10.10.11.50)
                Summary Link States (Area 0.0.0.0)
                Summary Link States (Area 0.0.0.1)
  LS age: 1124
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 10.10.10.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x41a2
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
```

Figure 28-15: Example output from the **show ip ospf database summary self-originate** command

```
       OSPF Router process 100 with ID (10.10.11.50)
                Summary Link States (Area 0.0.0.0)
  LS age: 1061
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
                Summary Link States (Area 0.0.0.1)
  LS age: 1061
  Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
                Summary Link States (Area 0.0.0.1)
  LS age: 1061
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 10.10.10.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x41a2
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
```

Figure 28-16: Example output from the **show ip ospf database summary adv-router <***ip-address***>** command

```
       OSPF Router process 100 with ID (10.10.11.50)
                Summary Link States (Area 0.0.0.0)
  LS age: 989
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
               Summary Link States (Area 0.0.0.1)
  LS age: 989
  Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
```

show ip ospf interface

Overview Use this command to display interface information for OSPF.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ip ospf interface [<interface-name>]
```

Parameter	Description
<interface-name>	The VLAN name, for example vlan3.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf interface vlan2
```

Output Figure 28-17: Example output from the **show ip ospf interface** command

```
vlan2 is up, line protocol is up
  Internet Address 1.1.1.1/24, Area 0.0.0.0, MTU 1500
  Process ID 0, Router ID 33.33.33.33, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State Waiting, Priority 1, TE Metric 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Neighbor Count is 0, Adjacent neighbor count is 0
  Crypt Sequence Number is 1106347721
  Hello received 0 sent 1, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
```

show ip ospf neighbor

Overview Use this command to display information on OSPF neighbors. Include the **ospf-id** parameter with this command to display information about specified instances.

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

Syntax

```
show ip ospf [<ospf-id>] neighbor <neighbor-ip-addr> [detail]
show ip ospf [<ospf-id>] neighbor detail [all]
show ip ospf [<ospf-id>] neighbor [all]
show ip ospf [<ospf-id>] neighbor interface <ip-addr>
```

Parameter	Description
<ospf-id>	<0-65535> The ID of the router process for which information will be displayed.
<neighbor-ip-addr>	The Neighbor ID, entered as an IP address.
`all`	Include downstatus neighbor.
`detail`	Detail of all neighbors.
<ip-addr>	IP address of the interface.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf neighbor detail
awplus# show ip ospf neighbor 1.2.3.4
awplus# show ip ospf neighbor interface 10.10.10.50 detail all
```

Output Note that before a device enters OSPF Graceful Restart it first informs its OSPF neighbors. In the **show** output, the * symbol beside the **Dead Time** parameter indicates that the device has been notified of a neighbor entering the graceful restart state, as shown in the figures below.

Figure 28-18: Example output from the **show ip ospf neighbor** command

```
OSPF process 1:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.50       1   Full/DR         00:00:38    10.10.10.50     vlan1
OSPF process 100:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.11.50       1   Full/Backup     00:00:31    10.10.11.50     vlan2
awplus#show ip ospf 1 neighbor
OSPF process 1:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.50       1   Full/DR         00:00:38*   10.10.10.50     vlan1
```

Figure 28-19: Example output from the **show ip ospf <ospf-id> neighbor** command

```
OSPF process 100:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.0.3      50   2-Way/DROther   00:01:59*   192.168.200.3   vlan200
```

Figure 28-20: Example output from the **show ip ospf neighbor detail** command

```
 Neighbor 10.10.10.50, interface address 10.10.10.50
    In the area 0.0.0.0 via interface vlan5
    Neighbor priority is 1, State is Full, 5 state changes
    DR is 10.10.10.50, BDR is 10.10.10.10
    Options is 0x42 (*|O|-|-|-|-|E|-)
    Dead timer due in 00:00:38
    Neighbor is up for 00:53:07
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Crypt Sequence Number is 0
    Thread Inactivity Timer on
    Thread Database Description Retransmission off
    Thread Link State Request Retransmission off
    Thread Link State Update Retransmission on
 Neighbor 10.10.11.50, interface address 10.10.11.50
    In the area 0.0.0.0 via interface vlan2
    Neighbor priority is 1, State is Full, 5 state changes
    DR is 10.10.11.10, BDR is 10.10.11.50
    Options is 0x42 (*|O|-|-|-|-|E|-)
    Dead timer due in 00:00:31
    Neighbor is up for 00:26:50
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Crypt Sequence Number is 0
    Thread Inactivity Timer on
    Thread Database Description Retransmission off
    Thread Link State Request Retransmission off
    Thread Link State Update Retransmission on
```

show ip ospf route

Overview Use this command to display the OSPF routing table. Include the **ospf-id** parameter with this command to display the OSPF routing table for specified instances.

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

Syntax

```
show ip ospf [<ospf-id>] route
```

Parameter	Description
<ospf-id>	<0-65535> The ID of the router process for which information will be displayed. If this parameter is included, only the information for this specified routing process is displayed.

Mode User Exec and Privileged Exec

Examples To display the OSPF routing table, use the command:

```
awplus# show ip ospf route
```

Output Figure 28-21: Example output from the **show ip ospf route** command for a specific process

```
OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
O  10.10.0.0/24 [10] is directly connected, vlan1, Area 0.0.0.0
O  10.10.11.0/24 [10] is directly connected, vlan2, Area 0.0.0.0
O  10.10.11.100/32 [10] is directly connected, lo, Area 0.0.0.0
E2 10.15.0.0/24 [10/50] via 10.10.0.1, vlan1
IA 172.16.10.0/24 [30] via 10.10.11.50, vlan2, Area 0.0.0.0
E2 192.168.0.0/16 [10/20] via 10.10.11.50, vlan2
```

show ip ospf virtual-links

Overview Use this command to display virtual link information.

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

Syntax

```
show ip ospf virtual-links
```

Mode User Exec and Privileged Exec

Examples To display virtual link information, use the command:

```
awplus# show ip ospf virtual-links
```

Output Figure 28-22: Example output from the **show ip ospf virtual-links** command

```
Virtual Link VLINK0 to router 10.10.0.9 is up
  Transit area 0.0.0.1 via interface vlan5
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in 00:00:02
    Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
  Transit area 0.0.0.1 via interface *
  Transmit Delay is 1 sec, State Down,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    Hello due in inactive
    Adjacency state Down
```

show ip protocols ospf

Overview Use this command to display OSPF process parameters and statistics.

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

Syntax

```
show ip protocols ospf
```

Mode User Exec and Privileged Exec

Examples To display OSPF process parameters and statistics, use the command:

```
awplus# show ip protocols ospf
```

Output Figure 28-23: Example output from the **show ip protocols ospf** command

```
Routing Protocol is "ospf 200"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is
    Redistributed kernel filtered by filter1
  Incoming update filter list for all interfaces is
  Redistributing: kernel
  Routing for Networks:
    192.30.30.0/24
    192.40.40.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
    Address         Mask            Distance List
```

summary-address

Overview Use this command to summarize, or possibly suppress, external routes that have the specified address range.

Use the **no** variant of this command to stop summarizing, or suppressing, external routes that have the specified address range.

Syntax

```
summary-address <ip-addr/prefix-length> [not-advertise] [tag <0-4294967295>]
```

```
no summary-address <ip-addr/prefix-length> [not-advertise] [tag <0-4294967295>]
```

Parameter	Description
<ip-addr/prefix-length>	Specifies the base IP address of the summary address.The range of addresses given as IPv4 starting address and a prefix length.
`not-advertise`	Set the **not-advertise** option if you do not want OSPF to advertise either the summary address or the individual networks within the range of the summary address.
`tag <0-4294967295>`	The tag parameter specifies the tag value that OSPF places in the AS external LSAs created as a result of redistributing the summary route. The tag overrides tags set by the original route.

Default The default tag value for a summary address is 0.

Mode Router Configuration

Usage notes An address range is a pairing of an address and a mask that is almost the same as IP network number. For example, if the specified address range is 192.168.0.0/255.255.240.0, it matches: 192.168.1.0/24, 192.168.4.0/22, 192.168.8.128/25 and so on.

Redistributing routes from other protocols into OSPF requires the router to advertise each route individually in an external LSA. Use the **summary address** command to advertise one summary route for all redistributed routes covered by a specified network address and mask. This helps decrease the size of the OSPF link state database.

Ensure OSPF routes exist in the summary address range for advertisement before using this command.

Example The following example uses the **summary-address** command to aggregate external LSAs that match the network 172.16.0.0/16 and assign a Tag value of 3.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# summary-address 172.16.0.0/16 tag 3
```

timers spf exp

Overview Use this command to adjust route calculation timers using exponential back-off delays.

Use **no** form of this command to return to the default exponential back-off timer values.

Syntax

```
timers spf exp <min-holdtime> <max-holdtime>
no timers spf exp
```

Parameter	Description
<min-holdtime>	*<0-2147483647>* Specifies the minimum delay between receiving a change to the SPF calculation in milliseconds. The default SPF min-holdtime value is 50 milliseconds.
<max-holdtime>	*<0-2147483647>* Specifies the maximum delay between receiving a change to the SPF calculation in milliseconds. The default SPF max-holdtime value is 50 seconds.

Mode Router Configuration

Default The default SPF min-holdtime is 50 milliseconds. The default SPF max-holdtime is 40 seconds.

Usage This command configures the minimum and maximum delay time between the receipt of a topology change and the calculation of the Shortest Path First (SPF).

Examples To set the minimum delay time to 5 milliseconds and maximum delay time to 10 milliseconds, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# timers spf exp 5 10
```

To reset the minimum and maximum delay times to the default values, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# no timers spf exp
```

Related commands timers spf exp

undebug ospf events

Overview This command applies the functionality of the no debug ospf events command.

undebug ospf ifsm

Overview This command applies the functionality of the no debug ospf ifsm command.

undebug ospf lsa

Overview This command applies the functionality of the no debug ospf lsa command.

undebug ospf nfsm

Overview This command applies the functionality of the no debug ospf nfsm command.

undebug ospf nsm

Overview This command applies the functionality of the no debug ospf nsm command.

undebug ospf packet

Overview This command applies the functionality of the no debug ospf packet command.

undebug ospf route

Overview This command applies the functionality of the no debug ospf route command.

29 OSPFv3 for IPv6 Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure OSPFv3 for IPv6. See the OSPFv3 Feature Overview and Configuration Guide for more information and examples.

Command List

- "abr-type" on page 1182
- "area authentication ipsec spi" on page 1183
- "area default-cost (IPv6 OSPF)" on page 1185
- "area encryption ipsec spi esp" on page 1186
- "area range (IPv6 OSPF)" on page 1189
- "area stub (IPv6 OSPF)" on page 1191
- "area virtual-link (IPv6 OSPF)" on page 1192
- "area virtual-link authentication ipsec spi" on page 1194
- "area virtual-link encryption ipsec spi" on page 1196
- "auto-cost reference bandwidth (IPv6 OSPF)" on page 1199
- "bandwidth" on page 1201
- "clear ipv6 ospf process" on page 1202
- "debug ipv6 ospf events" on page 1203
- "debug ipv6 ospf ifsm" on page 1204
- "debug ipv6 ospf lsa" on page 1205
- "debug ipv6 ospf nfsm" on page 1206
- "debug ipv6 ospf packet" on page 1207
- "debug ipv6 ospf route" on page 1208
- "default-information originate" on page 1209

- "default-metric (IPv6 OSPF)" on page 1210
- "distance (IPv6 OSPF)" on page 1211
- "distribute-list (IPv6 OSPF)" on page 1213
- "ipv6 ospf authentication spi" on page 1215
- "ipv6 ospf cost" on page 1217
- "ipv6 ospf dead-interval" on page 1218
- "ipv6 ospf display route single-line" on page 1219
- "ipv6 ospf encryption spi esp" on page 1220
- "ipv6 ospf hello-interval" on page 1223
- "ipv6 ospf neighbor" on page 1224
- "ipv6 ospf network" on page 1226
- "ipv6 ospf priority" on page 1227
- "ipv6 ospf retransmit-interval" on page 1228
- "ipv6 ospf transmit-delay" on page 1229
- "ipv6 router ospf area" on page 1230
- "max-concurrent-dd (IPv6 OSPF)" on page 1232
- "passive-interface (IPv6 OSPF)" on page 1233
- "redistribute (IPv6 OSPF)" on page 1234
- "restart ipv6 ospf graceful" on page 1236
- "router ipv6 ospf" on page 1237
- "router-id (IPv6 OSPF)" on page 1238
- "show debugging ipv6 ospf" on page 1239
- "show ipv6 ospf" on page 1240
- "show ipv6 ospf database" on page 1242
- "show ipv6 ospf database external" on page 1244
- "show ipv6 ospf database grace" on page 1245
- "show ipv6 ospf database inter-prefix" on page 1246
- "show ipv6 ospf database inter-router" on page 1247
- "show ipv6 ospf database intra-prefix" on page 1248
- "show ipv6 ospf database link" on page 1249
- "show ipv6 ospf database network" on page 1250
- "show ipv6 ospf database router" on page 1252
- "show ipv6 ospf interface" on page 1257
- "show ipv6 ospf neighbor" on page 1259
- "show ipv6 ospf route" on page 1261

- "show ipv6 ospf virtual-links" on page 1263
- "summary-address (IPv6 OSPF)" on page 1264
- "timers spf exp (IPv6 OSPF)" on page 1266
- "undebug ipv6 ospf events" on page 1267
- "undebug ipv6 ospf ifsm" on page 1268
- "undebug ipv6 ospf lsa" on page 1269
- "undebug ipv6 ospf nfsm" on page 1270
- "undebug ipv6 ospf packet" on page 1271
- "undebug ipv6 ospf route" on page 1272

abr-type

Overview Use this command to set an OSPF Area Border Router (ABR) type.

Use the **no** variant of this command to revert the ABR type to the default setting (cisco).

Syntax

```
abr-type {cisco|ibm|standard}
no abr-type {cisco|ibm|standard}
```

Parameter	Description
`cisco`	Specifies an alternative ABR using Cisco implementation (RFC 3509). This is the default ABR type.
`ibm`	Specifies an alternative ABR using IBM implementation (RFC 3509).
`standard`	Specifies a standard behavior ABR (RFC 2328).

Default ABR type cisco

Mode Router Configuration

Usage notes Specifying the ABR type allows better interoperation between different implementations. This command is specially useful in a multi-vendor environment. The different ABR types are:

- Cisco ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached and one of them is the backbone area.
- IBM ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached and the backbone area is configured. In this case the configured backbone need not be actively connected.
- Standard ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached to it.

Example To set the ABR type to “ibm” use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# abr-type ibm
```

area authentication ipsec spi

Overview Use this command in Router Configuration mode to enable either MD5 (Message-Digest 5) or SHA1 (Secure Hash Algorithm 1) authentication for a specified OSPF area.

Use the **no** variant of this command in Router Configuration mode to disable the authentication configured for a specified OSPF area.

Syntax

```
area <area-id> authentication ipsec spi <256-4294967295> {md5 <MD5-key>|sha1 <SHA1-key>}
no area <area-id> authentication ipsec spi <256-4294967295>
```

Parameter	Description	
<area-id>	The OSPF area that you are specifying the summary route default-cost for. This can be entered in either dotted decimal format or normal decimal format. Use one of the following formats:	
	<ip-addr>	OSPF area-ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295>	OSPF area-ID expressed as a decimal number within the range shown.
	For example, the values 0.0.1.2 and decimal 258 would both define the same area-ID.	
<256-4294967295>	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.	
md5	Specify the MD5 (Message-Digest 5) hashing algorithm.	
<MD5-key>	Enter an MD5 key containing up to 32 hexadecimal characters.	
sha1	Specify the SHA-1 (Secure Hash Algorithm 1) hashing algorithm.	
<SHA1-key>	Enter an SHA-1 key containing up to 40 hexadecimal characters.	

Mode Router Configuration

Usage notes Use this command on an OSPFv3 area; use the area virtual-link authentication ipsec spi command on an OSPFv3 area virtual link. Configure the same SPI (Security Parameters Index) value on all interfaces that connect to the same link. SPI values are used by link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

See the OSPFv3 Feature Overview and Configuration Guide for more information and examples.

NOTE: *You can configure an authentication security policy (SPI) on an OSPFv3 area with this command, or on a VLAN interface with the ipv6 ospf authentication spi command.*

When you configure authentication for an area, the security policy is applied to all VLAN interfaces in the area. However, we recommend a different authentication security policy is applied to each interface for higher security.

If you apply the ***ipv6 ospf authentication null*** *command, this affects authentication configured on both the VLAN interface and the OSPFv3 area.*

This is due to OSPFv3 hello messages ingressing VLAN interfaces, which are part of area authentication, not being authenticated. So neighbors time out.

Example To enable MD5 authentication with a 32 hexadecimal character key for OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 authentication ipsec spi 1000 md5
1234567890ABCDEF1234567890ABCDEF
```

To enable SHA-1 authentication with a 40 hexadecimal character key for OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 authentication ipsec spi 1000
sha1 1234567890ABCDEF1234567890ABCDEF12345678
```

To disable authentication for OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no area 1 authentication ipsec spi 1000
```

Related commands

area encryption ipsec spi esp

area virtual-link authentication ipsec spi

area virtual-link encryption ipsec spi

ipv6 ospf authentication spi

ipv6 ospf encryption spi esp

show ipv6 ospf

area default-cost (IPv6 OSPF)

Overview This command specifies a cost for the default summary route sent into a stub area.

The **no** variant of this command removes the assigned default-route cost.

Syntax

```
area <area-id> default-cost <0-16777215>
no area <area-id> default-cost
```

Parameter	Description	
<area-id>	The OSPF area that you are specifying the summary route default-cost for. This can be entered in either dotted decimal format or normal decimal format. Use one of the following formats:	
	<ip-addr>	OSPF area-ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295>	OSPF area-ID expressed as a decimal number within the range shown.
	For example, the values 0.0.1.2 and decimal 258 would both define the same area-ID.	
`default-cost`	Indicates the cost for the default summary route used for a stub area. Default: **1**	

Mode Router Configuration

Usage The default-cost option provides the metric for the summary default route, generated by the area border router, into the stub area. Use this option only on an area border router that is attached to the stub area.

Example To set the default cost to 10 in area 1 for the OSPF process P2, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf P2
awplus(config-router)# area 1 default-cost 10
```

Related commands area stub (IPv6 OSPF)

area encryption ipsec spi esp

Overview Use this command in Router Configuration mode to enable either AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) or 3DES (Triple Data Encryption Standard) ESP (Encapsulating Security Payload) encryption for a specified OSPF area.

Use the **no** variant of this command in Router Configuration mode to disable the encryption configured for a specified OSPF area.

Syntax

```
area <area-id> encryption ipsec spi <256-4294967295> esp
{aes-cbc <AES-CBC-key>|3des <3DES-key>|null}{md5
<MD5-key>|sha1 <SHA1-key>}
```

```
no area <area-id> encryption ipsec spi <256-4294967295>
```

Parameter	Description	
<area-id>	The OSPF area that you are specifying the summary route default-cost for. This can be entered in either dotted decimal format or normal decimal format. Use one of the following formats:	
	<ip-addr>	OSPF area-ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295>	OSPF area-ID expressed as a decimal number within the range shown.
	For example, the values 0.0.1.2 and decimal 258 would both define the same area-ID.	
<256-4294967295>	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.	
esp	Specify the esp keyword (Encapsulating Security Payload) to then apply either AES-CBC or 3DES encryption.	
aes-cbc	Specify this keyword to enable AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) encryption.	
<AES-CBC-key>	Enter an AES-CBC key containing either 32, 48, or 64 hexadecimal characters.	
3des	Specify 3DES (Triple Data Encryption Standard) encryption.	
<3DES-key>	Enter a 3DES key containing 48 hexadecimal characters.	
null	Specify ESP without AES-CBC or 3DES encryption applied.	
md5	Specify the MD5 (Message-Digest 5) encryption algorithm.	
<MD5-key>	Enter an MD5 key containing 32 hexadecimal characters.	
sha1	Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.	
<SHA1-key>	Enter an SHA-1 key containing 40 hexadecimal characters.	

Mode Router Configuration

Usage notes

When you issue this command, authentication and encryption are both enabled.

Use this command on an OSPFv3 area, use the area virtual-link encryption ipsec spi command on an OSPFv3 area virtual link. Configure the same SPI (Security Parameters Index) value on all interfaces that connect to the same link. SPI values are used by link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

Security is achieved using the IPv6 ESP extension header. The IPv6 ESP extension header is used to provide confidentiality, integrity, authentication, and confidentiality. Authentication fields are removed from OSPF for IPv6 packet headers, so applying IPv6 ESP extension headers are required for integrity, authentication, and confidentiality.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

See the OSPFv3 Feature Overview and Configuration Guide for more information and examples.

NOTE: *You can configure an encryption security policy (SPI) on an OSPFv3 area with this command, or on a VLAN interface with the ipv6 ospf encryption spi esp command.*

When you configure encryption for an area, the security policy is applied to all VLAN interfaces in the area. However, we recommend a different encryption security policy is applied to each interface for higher security.

*If you apply the **ipv6 ospf encryption null** command, this affects encryption configured on both the VLAN interface and the OSPFv3 area.*

This is due to OSPFv3 hello messages ingressing VLAN interfaces, which are part of area encryption, not being being encrypted. So neighbors time out.

Example

To enable ESP encryption, but not apply an AES-CBC key or an 3DES key, and MD5 authentication with a 32 hexadecimal character key for OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 encryption ipsec spi 1000 esp null
md5 1234567890ABCDEF1234567890ABCDEF
```

To enable ESP encryption, but not apply an AES-CBC key or an 3DES key, and SHA-1 authentication with a 40 hexadecimal character key for OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 encryption ipsec spi 1000 esp null
sha1 1234567890ABCDEF1234567890ABCDEF12345678
```

To enable ESP encryption with a 48 hexadecimal character 3DES key and a 32 hexadecimal character MD5 authentication for OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 encryption ipsec spi 1000 esp 3des
1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF md5
1234567890ABCDEF1234567890ABCDEF
```

To enable ESP encryption with a 32 hexadecimal character AES-CBC key, and a 40 hexadecimal character SHA-1 authentication key for OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 encryption ipsec spi 1000 esp
aes-cbc 1234567890ABCDEF1234567890ABCDEF sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To disable ESP encryption for OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no area 1 encryption ipsec spi 1000
```

Related commands

area authentication ipsec spi

area virtual-link authentication ipsec spi

area virtual-link encryption ipsec spi

ipv6 ospf authentication spi

ipv6 ospf encryption spi esp

show ipv6 ospf

area range (IPv6 OSPF)

Overview Use this command to summarize OSPFv3 routes at an area boundary, configuring an IPv6 address range which consolidates OSPFv3 routes. By default, this feature is not enabled.

A summary route created by this command is then advertised to other areas by the Area Border Routers (ABRs). In this way, routing information is condensed at area boundaries and outside the area so that routes are exchanged between areas in an efficient manner.

If the network numbers in an area are arranged into sets of contiguous routes, the ABRs can be configured to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

The **no** variant of this command disables this function and restores default behavior.

Syntax

```
area <area-id> range <ipv6address/prefix-length>
[advertise|not-advertise]
```

```
no area <area-id> range <ipv6address/prefix-length>
```

Parameter	Description	
<area-id>	The OSPFv3 area that you summarizing the routes for. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format.	
	<A.B.C.D>	OSPF area-ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295>	OSPF area-ID expressed as a decimal number within the range shown.
	For example the values 0.0.1.2 and decimal 258 would both define the same area-ID.	
<ip-addr/ prefix-length>	The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.	
`advertise`	Advertise this range as a summary route into other areas.	
`not-advertise`	Do not advertise this range.	

Default The area range is not configured by default. The area range is advertised if it is configured.

Mode Router Configuration

Usage notes You can configure multiple ranges on a single area with multiple instances of this command, so OSPFv3 summarizes addresses for different sets of IPv6 address ranges.

Ensure OSPFv3 IPv6 routes exist in the area range for advertisement before using this command.

Example

```
awplus# configure terminal
awplus(config)# router ipv6 ospf P2
awplus(config-router)# area 1 range 2000::/3
```

area stub (IPv6 OSPF)

Overview This command defines an OSPF area as a stub area. By default, no stub area is defined.

Use this command when routers in the area do not require learning about external LSAs. You can define the area as a totally stubby area by configuring the Area Border Router of that area using the **area stub no-summary** command.

The **no** variant of this command removes this definition.

Syntax

```
area <area-id> stub [no-summary]
no area <area-id> stub [no-summary]
```

Parameter	Description	
<area-id>	The OSPF area that you are configuring as a stub area. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format. For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area-ID.	
	<A.B.C.D>	OSPF area-ID, expressed in the IPv4 address format *<A.B.C.D>*.
	<0-4294967295>	OSPF area-ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area-ID.	
no-summary	Stops an ABR from sending summary link advertisements into the stub area.	

Mode Router Configuration

Usage There are two stub area router configuration commands: the **area stub** and **area default- cost** commands. In all routers attached to the stub area, configure the area by using the **area stub** command. For an area border router (ABR) attached to the stub area, also use the **area default-cost** command.

Example

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# area 100 stub
```

Related commands area default-cost (IPv6 OSPF)

area virtual-link (IPv6 OSPF)

Overview This command configures a link between a non-backbone area and the backbone, through other non-backbone areas.

In OSPF, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection.

The **no** variant of this command removes the virtual link.

Syntax

```
area <area-id> virtual-link <router-id>
no area <area-id>  virtual-link <router-id>
area <area-id>  virtual-link <router-id>
no area <area-id>  virtual-link <router-id>
area <area-id>  virtual-link <router-id> [hello-interval <1-65535>]  [retransmit-interval <1-65535>] [transmit-delay <1-65535>]
no area <area-id>  virtual-link <router-id> [hello-interval] [retransmit-interval] [transmit-delay]
```

Parameter	Description	
<area-id>	The area-ID of the transit area that the virtual link passes through. This can be entered in either dotted decimal format or normal decimal format as shown below.	
	<A.B.C.D>	OSPF area-ID, expressed in the IPv4 address format *<A.B.C.D>*.
	<0-4294967295>	OSPF area-ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area-ID.	
<router-id>	The OSPF router ID of the virtual link neighbor.	
dead-interval	If no packets are received from a particular neighbor for dead-interval seconds, the router considers the neighbor router to be off-line. Default: 40 seconds	
	<1-65535>	The number of seconds in the interval.
hello-interval	The interval the router waits before it sends a hello packet. Default: 10 seconds	
	<1-65535>	The number of seconds in the interval.
retransmit-interval	The interval the router waits before it retransmits a packet. Default: 5 seconds	
	<1-65535>	The number of seconds in the interval.

Parameter	Description	
`transmit-delay`	The interval the router waits before it transmits a packet. Default: 1 seconds	
	<1-65535>	The number of seconds in the interval.

Mode Router Configuration

Usage You can configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these two routers, joined by a virtual link, as if they were connected by an unnumbered point-to-point network. To configure a virtual link, you require:

- The transit area-ID, i.e. the area-ID of the non-backbone area that the two backbone routers are both connected to.
- The corresponding virtual link neighbor's router ID. To see the router ID use the show ipv6 ospf command.

Configure the **hello-interval** to be the same for all routers attached to a common network. A short **hello-interval** results in the router detecting topological changes faster but also an increase in the routing traffic.

The **retransmit-interval** is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The **transmit-delay** is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet, are incremented by this amount. Set the **transmit-delay** to be greater than zero. Also, take into account the transmission and propagation delays for the interface.

Example To configure a virtual link through area 1to the router with router-ID 10.10.11.50, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# area 1 virtual-link 10.10.11.50 hello 5
dead 10
```

Related commands show ipv6 ospf

area virtual-link authentication ipsec spi

Overview Use this command in Router Configuration mode to enable authentication for virtual links in a specified OSPF area.

Use the **no** variant of this command in Router Configuration mode to disable authentication for virtual links in a specified OSPF area.

Syntax

```
area <area-id> virtual-link <router-ID> authentication ipsec
spi <256-4294967295> {md5 <MD5-key>|sha1 <SHA1-key>}
```

```
no area <area-id> virtual-link <router-ID> authentication ipsec
spi <256-4294967295>
```

Parameter	Description	
<area-id>	The OSPF area that you are specifying the summary route default-cost for. This can be entered in either dotted decimal format or normal decimal format. Use one of the following formats:	
	<ip-addr>	OSPF area-ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295>	OSPF area-ID expressed as a decimal number within the range shown.
	For example, the values 0.0.1.2 and decimal 258 would both define the same area-ID.	
`virtual-link`	Specify a virtual link and its parameters.	
<router-ID>	Enter a router ID associated with a virtual link neighbor in IPv4 address format A.B.C.D.	
`authentication`	Specify this keyword to enable authentication.	
`ipsec`	Specify this keyword to use IPsec authentication.	
`spi`	Specify this keyword to set the SPI (Security Parameters Index).	
<256-4294967295>	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.	
`md5`	Specify the MD5 (Message-Digest 5) encryption algorithm.	
<MD5-key>	Enter an MD5 key containing 32 hexadecimal characters.	
`sha1`	Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.	
<SHA1-key>	Enter an SHA-1 key containing 40 hexadecimal characters.	

Mode Router Configuration

Usage notes Use this command on an OSPFv3 area virtual link, use the area authentication ipsec spi command on an OSPFv3 area. Configure the same SPI (Security Parameters Index) value on all interfaces that connect to the same link. SPI values are used by

link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

OSPFv3 areas are connected to a backbone area. Virtual links can be configured to repair lost connections to a backbone area for OSPFv3 areas. To configure an OSPFv3 virtual link, use a router ID instead of the IPv6 prefix of the router.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

See the OSPFv3 Feature Overview and Configuration Guide for more information and examples.

Example To enable MD5 authentication with a 32 hexadecimal character key for virtual links in OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1
authentication ipsec spi 1000 md5
1234567890ABCDEF1234567890ABCDEF
```

To enable SHA-1 authentication with a 40 hexadecimal character key for virtual links in OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1
authentication ipsec spi 1000 sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To disable authentication for virtual links in OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no area 1 virtual-link ipsec spi 1000
```

Related commands

area authentication ipsec spi

area encryption ipsec spi esp

area virtual-link encryption ipsec spi

show ipv6 ospf virtual-links

area virtual-link encryption ipsec spi

Overview Use this command in Router Configuration mode to enable either AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) or 3DES (Triple Data Encryption Standard) ESP (Encapsulating Security Payload) encryption for virtual links in a specified OSPF area.

Use the **no** variant of this command in Router Configuration mode to disable encryption configured for virtual links in a specified OSPF area.

Syntax

```
area <area-id> virtual-link <router-ID> encryption ipsec spi
<256-4294967295> esp {aes-cbc <AES-CBC-key>|3des
<3DES-key>|null}{md5 <MD5-key>|sha1 <SHA1-key>}
```

```
no area <area-id> encryption ipsec spi <256-4294967295>
```

Parameter	Description	
<area-id>	The OSPF area that you are specifying the summary route default- cost for. This can be entered in either dotted decimal format or normal decimal format. Use one of the following formats:	
	<ip-addr>	OSPF area-ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295>	OSPF area-ID expressed as a decimal number within the range shown.
	For example, the values 0.0.1.2 and decimal 258 would both define the same area-ID.	
`virtual-link`	Specify a virtual link and its parameters.	
<router-ID>	Enter a router ID associated with a virtual link neighbor in IPv4 address format A.B.C.D.	
`encryption`	Specify this keyword to enable encryption.	
`ipsec`	Specify this keyword to use IPsec authentication.	
`spi`	Specify this keyword to set the SPI (Security Parameters Index).	
<256-4294967295>	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.	
`esp`	Specify the esp keyword (Encapsulating Security Payload) to then apply either AES-CBC or 3DES encryption.	
`aes-cbc`	Specify this keyword to enable AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) encryption.	
<AES-CBC-key>	Enter an AES-CBC key containing either 32, 48, or 64 hexadecimal characters.	
`3des`	Specify 3DES (Triple Data Encryption Standard) encryption.	
<3DES-key>	Enter a 3DES key containing 48 hexadecimal characters.	

Parameter	Description
`null`	Specify ESP without AES-CBC or 3DES encryption applied.
`md5`	Specify the MD5 (Message-Digest 5) encryption algorithm.
<MD5-key>	Enter an MD5 key containing 32 hexadecimal characters.
`sha1`	Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.
<SHA1-key>	Enter an SHA-1 key containing 40 hexadecimal characters.

Mode Router Configuration

Usage notes When you issue this command, authentication and encryption are both enabled.

Use this command on an OSPFv3 area virtual link, use the area encryption ipsec spi esp command on an OSPFv3 area. Configure the same SPI (Security Parameters Index) value on all interfaces that connect to the same link. SPI values are used by link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

Security is achieved using the IPv6 ESP extension header. ESP is used to provide confidentiality, integrity, authentication, and confidentiality. Authentication fields are removed from OSPF for IPv6 packet headers. The IPv6 ESP extension header is required for integrity, authentication, and confidentiality.

Note that interface configuration takes priority over area configuration. If an interface configuration is removed then an area configuration is applied to an interface instead.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

See the OSPFv3 Feature Overview and Configuration Guide for more information and examples.

Example To enable ESP encryption, but not apply an AES-CBC key or a 3DES key, and MD5 authentication with a 32 hexadecimal character key for virtual links in OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1 encryption
ipsec spi 1000 esp null md5 1234567890ABCDEF1234567890ABCDEF
```

To enable ESP encryption, but not apply an AES-CBC key or a 3DES key, and SHA-1 authentication with a 40 hexadecimal character key for virtual links in OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1 encryption
ipsec spi 1000 esp null sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To enable ESP encryption with a 32 hexadecimal character AES-CBC key and a 40 hexadecimal character SHA-1 authentication key for virtual links in OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1 encryption
ipsec spi 1000 esp aes-cbc 1234567890ABCDEF1234567890ABCDEF
sha1 1234567890ABCDEF1234567890ABCDEF12345678
```

To enable ESP encryption with a 48 hexadecimal character 3DES key and a 40 hexadecimal character SHA-1 authentication key for virtual links in OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1 encryption
ipsec spi 1000 esp 3des
1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To disable authentication for virtual links in OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no area 1 virtual-link 10.0.0.1
authentication ipsec spi 1000
```

Related commands

area authentication ipsec spi

area encryption ipsec spi esp

area virtual-link authentication ipsec spi

show ipv6 ospf virtual-links

auto-cost reference bandwidth (IPv6 OSPF)

Overview This command controls how OSPF calculates default metrics for the interface.

Use the **no** variant of this command to assign cost based only on the interface bandwidth.

Syntax

```
auto-cost reference-bandwidth <1-4294967>
no auto-cost reference-bandwidth
```

Parameter	Description
<1-4294967>	The reference bandwidth, measured in Mbits per second (Mbps).

Default 1000 Mbps

Usage notes By default, OSPF calculates the OSPF metric for an interface by dividing the reference bandwidth by the interface bandwidth. The default for the reference bandwidth is 1000 Mbps. As a result, if this default is used, there is very little difference between the metrics applied to interfaces of increasing bandwidth beyond 1000 Mbps.

The auto-cost command is used to alter this reference bandwidth in order to give a real difference between the metrics of high bandwidth links of differing bandwidths. In a network that has multiple links with high bandwidths, specify a larger reference bandwidth value to differentiate the costs on those links.

Cost is calculated by dividing the reference bandwidth (Mbps) by the layer 3 interface (Switched Virtual Interface (SVI), Loopback or Ethernet interface) bandwidth. Interface bandwidth may be altered by using the bandwidth command as the SVI does not auto-detect the bandwidth based on the speed of associated device ports.

When the reference bandwidth calculation results in a cost integer greater than 1 but contains a fractional value (the value after the decimal point), the result rounds down to the nearest integer. The following example shows how the cost is calculated.

The reference bandwidth is 1000 Mbps and the interface bandwidth is 7 Mbps.

Calculation = 1000/7

Calculation result = 142.85 (integer of 142, fractional value of 0.85)

Result after rounding down to the nearest integer = 142 (Interface cost is 142)

When the reference bandwidth calculation results in a cost less than 1, it is rounded up to the nearest integer which is 1. The following example shows how the cost is calculated.

The reference bandwidth is 1000 Mbps and the interface bandwidth is 10000 Mbps.

Calculation = 1000/10000

Calculation result = 0.1

Result after rounding up to the nearest integer = 1 (Interface cost is 1)

The auto-cost reference bandwidth value should be consistent across all OSPF routers in the OSPF process.

Note that using the ipv6 ospf cost command on a layer 3 interface will override the cost calculated by this command.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 20
awplus(config-router)# auto-cost reference-bandwidth 1000
```

Related commands ipv6 ospf cost

bandwidth

Overview Use this command to specify the maximum bandwidth to be used for each VLAN interface. The bandwidth value is in bits per second. OSPF uses this to calculate metrics for the VLAN interface.

The **no** variant of this command removes any applied bandwidth value and replaces it with a value equal to the lowest port speed within that VLAN.

Syntax

```
bandwidth  <bandwidth-setting>
no bandwidth
```

Parameter	Description
<bandwidth-setting>	Sets the bandwidth for the interface. Enter a value in the range 1 to 10000000000 bits per second. Note that to avoid entering many zeros, you can add k, m, or g to internally add 3, 6 or 9 zeros to the number entered. For example entering 1k is the same as entering 1000.

Mode Interface Configuration for a VLAN interface.

Example To set the bandwidth on VLAN2 to be 1 Mbps, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# bandwidth 1000000
```

Or

```
awplus(config-if)# bandwidth 1m
```

Related commands show running-config access-list

show interface

clear ipv6 ospf process

Overview This command clears and restarts the IPv6 OSPF routing process. Specify the Process ID to clear one particular OSPF process. When no Process ID is specified, this command clears all running OSPF processes.

Syntax

```
clear ipv6 ospf [<0-65535>] process
```

Parameter	Description
<0-65535>	The routing process ID.

Mode Privileged Exec

Example

```
awplus# clear ipv6 ospf process
```

debug ipv6 ospf events

Overview This command enables IPv6 OSPF debugging for event troubleshooting.

To enable all debugging options, specify **debug ipv6 ospf event** with no additional parameters.

The **no** and **undebug** variants of this command disable OSPF debugging. Using this command with no parameters entered, will disable debugging for all parameter options.

Syntax

```
debug ipv6 ospf events [abr] [asbr] [os][router] [vlink]
no debug ipv6 ospf events [abr] [asbr] [os] [router] [vlink]
```

Parameter	Description
`abr`	Shows ABR events.
`asbr`	Shows ASBR events.
`router`	Shows other router events.
`os`	Shows OS events.
`vlink`	Shows virtual link events.

Mode Privileged Exec and Global Configuration

Example To enable IPv6 event debugging and show ABR events, use the following command:

```
awplus# debug ipv6 ospf events asbr
```

debug ipv6 ospf ifsm

Overview This command specifies debugging options for IPv6 OSPF Interface Finite State Machine (IFSM) troubleshooting.

To enable all debugging options, specify **debug ipv6 ospf ifsm** with no additional parameters.

The **no** and **undebug** variants of this command disable IPv6 OSPF IFSM debugging. Use these commands without parameters to disable all the options.

Syntax

```
debug ipv6 ospf ifsm [events] [status] [timers]
no debug ipv6 ospf ifsm [events] [status] [timers]
```

Parameter	Description
`events`	Displays IFSM event information.
`status`	Displays IFSM status information.
`timers`	Displays IFSM timer information.

Mode Privileged Exec and Global Configuration

Example To specify IPv6 OSPF debugging options to display IPv6 OSPF IFSM events information, use the following commands:

```
awplus# debug ipv6 ospf ifsm events
```

Related commands terminal monitor

undebug ipv6 ospf ifsm

debug ipv6 ospf lsa

Overview This command enables debugging options for IPv6 OSPF Link State Advertisements (LSA) troubleshooting. This displays information related to internal operations of LSAs.

To enable all debugging options, specify **debug ipv6 ospf lsa** with no additional parameters.

The **no** and **undebug** variants of this command disable IPv6 OSPF LSA debugging. Use this command without parameters to disable all the options.

Syntax

```
debug ipv6 ospf lsa [flooding] [generate] [install] [maxage]
[refresh]
```

```
no debug ipv6 ospf lsa [flooding] [generate] [install] [maxage]
[refresh]
```

Parameter	Description
`flooding`	Displays LSA flooding.
`generate`	Displays LSA generation.
`install`	Show LSA installation.
`maxage`	Shows maximum age of the LSA in seconds.
`refresh`	Displays LSA refresh.

Mode Privileged Exec and Global Configuration

Examples To enable debugging for IPv6 OSPF refresh LSA, use the following commands:

```
awplus# debug ipv6 ospf lsa refresh
```

Related commands terminal monitor

undebug ipv6 ospf lsa

debug ipv6 ospf nfsm

Overview This command enables debugging options for IPv6 OSPF Neighbor Finite State Machines (NFSMs).

To enable all debugging options, specify **debug ipv6 ospf nfsm** with no additional parameters.

The **no** and **undebug** variants of this command disable IPv6 OSPF NFSM debugging. Use this command without parameters to disable all the options.

Syntax

```
debug ipv6 ospf nfsm [events] [status] [timers]
no debug ipv6 ospf nfsm [events] [status] [timers]
```

Parameter	Description
`events`	Displays NFSM event information.
`status`	Displays NSFM status information.
`timers`	Displays NFSM timer information.

Mode Privileged Exec and Global Configuration

Examples To enable IPv6 debugging option to display timer information, use the following command:

```
awplus# debug ipv6 ospf nfsm timers
```

Related commands terminal monitor

undebug ipv6 ospf nfsm

debug ipv6 ospf packet

Overview This command enables debugging options for IPv6 OSPF packets.

To enable all debugging options, specify **debug ipv6 ospf packet** with no additional parameters.

The **no** and **undebug** variants of this command disable IPv6 OSPF packet debugging. Use this command without parameters to disable all options.

Syntax

```
debug ipv6 ospf packet [dd] [detail] [hello] [ls-ack]
[ls-request] [ls-update] [recv] [send]
```

```
no debug ipv6 ospf packet [dd] [detail] [hello] [ls-ack]
[ls-request] [ls-update] [recv] [send]
```

Parameter	Description
`dd`	Specifies debugging for IPv6 OSPF database descriptions.
`detail`	Sets the debug option to detailed information.
`hello`	Specifies debugging for IPv6 OSPF hello packets.
`ls-ack`	Specifies debugging for IPv6 OSPF link state acknowledgments.
`ls-request`	Specifies debugging for IPv6 OSPF link state requests.
`ls-update`	Specifies debugging for IPv6 OSPF link state updates.
`recv`	Specifies the debug option set for received packets.
`send`	Specifies the debug option set for sent packets.

Mode Privileged Exec and Global Configuration

Examples To enable debugging for hello packets, use the following command:

```
awplus# debug ipv6 ospf packet hello
```

Related commands terminal monitor

undebug ipv6 ospf packet

debug ipv6 ospf route

Overview This command enables debugging of route calculation. Use this command without parameters to turn on all the options.

The **no** and **undebug** variants of this command disable IPv6 OSPF route debugging. Use this command without parameters to disable all options.

Syntax

```
debug ipv6 ospf route [ase] [ia] [install] [spf]
no debug ipv6 ospf route [ase] [ia] [install] [spf]
```

Parameter	Description
`ase`	Specifies the debugging of external route calculation.
`ia`	Specifies the debugging of inter-area route calculation.
`install`	Specifies the debugging of route installation.
`spf`	Specifies the debugging of SPF calculation.

Mode Privileged Exec and Global Configuration

Examples To enable IPv6 route debugging of inter-area route calculations, use the following command:

```
awplus# debug ipv6 ospf route ia
```

Related commands terminal monitor

undebug ipv6 ospf route

default-information originate

Overview This command creates a default external route into an OSPF routing domain.

When you use the **default-information originate** command to redistribute routes into an OSPF routing domain, then the system acts like an Autonomous System Boundary Router (ASBR). By default, an ASBR does not generate a default route into the OSPF routing domain.

When using this command, also specify the **route-map** <*route-map*> option to avoid a dependency on the default network in the routing table.

The **metric-type** is an external link type associated with the default route advertised into the OSPF routing domain. The value of the external route could be either Type 1 or 2. The default is Type 2.

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

Syntax

```
default-information originate [always] [metric <metric>]
[metric-type <1-2>] [route-map <route-map>]
```

```
no default-information originate [always] [metric]
[metric-type] [route-map]
```

Parameter	Description
`always`	Used to advertise the default route regardless of whether there is a default route.
<metric>	The metric value used in creating the default route. Enter a value in the range 0 to 16777214. The default metric value is 10. The value used is specific to the protocol.
<1-2>	External metric type for default routes, either OSPF External Type 1 or Type 2 metrics. Enter the value 1 or 2.
`route-map`	Specifies to use a specific route-map.
<route-map>	The route-map name. It is a string comprised of any characters, numbers or symbols.

Mode Router Configuration

Example

```
awplus# configure terminal
```

```
awplus(config)# router ospf 100
```

```
awplus(config-router)# default-information originate always
metric 23 metric-type 2 route-map myinfo
```

Related commands route-map

default-metric (IPv6 OSPF)

Overview This command sets default metric value for routes redistributed into the IPv6 OSPF routing protocol.

The **no** variant of this command returns IPv6 OSPF to using built-in, automatic metric translations, as appropriate for each routing protocol.

Syntax

```
default-metric <0-16777214>
no default-metric [<0-16777214>]
```

Parameter	Description
<1-16777214>	Default metric value appropriate for the specified routing protocol.

Mode Router Configuration

Usage notes A default metric facilitates redistributing routes even with incompatible metrics. If the metrics do not convert, the default metric provides an alternative and enables the redistribution to continue. The effect of this command is that IPv6 OSPF will use the same metric value for **all** redistributed routes. Use this command in conjunction with the redistribute (IPv6 OSPF) command.

Examples

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# default-metric 100
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# no default-metric
```

Related commands redistribute (IPv6 OSPF)

distance (IPv6 OSPF)

Overview This command sets the administrative distance for OSPFv3 routes based on the route type. Your device uses this value to select between two or more routes to the same destination from two different routing protocols. The route with the smallest administrative distance value is added to the Forwarding Information Base (FIB). See the OSPFv3 Feature Overview and Configuration Guide for more information.

Use the command **distance ospfv3** to set the distance for an entire category of OSPFv3 routes, rather than the specific routes that pass an access list.

Use the command **distance <1-254>**, with no other parameter, to set the same distance for all OSPFv3 route types.

The **no** variant of this command sets the administrative distance for OSPFv3 routes to the default of 110.

Syntax

```
distance <1-254>
distance ospfv3 {external <1-254>|inter-area <1-254>|intra-area <1-254>}
no distance {ospfv3|<1-254>}
```

Parameter	Description
<1-254>	Specify the Administrative Distance value for OSPFv3 routes.
`external`	Sets the distance for routes from other routing domains, learned by redistribution. Specify an OSPFv3 external distance in the range *<1-254>*.
`inter-area`	Sets the distance for all routes from one area to another area. Specify an OSPFv3 inter-area distance in the range*<1-254>*.
`intra-area`	Sets the distance for all routes within an area. Specify an OSPFv3 intra-area distance in the range *<1-254>*.

Default The default OSPFv3 administrative distance is 110. The default Administrative Distance for each type of route (intra, inter, or external) is 110.

Mode Router Configuration

Usage notes The administrative distance rates the trustworthiness of a routing information source. The distance could be any integer from 0 to 254. A higher distance value indicates a lower trust rating. For example, an administrative distance of 254 indicates that the routing information source cannot be trusted and should be ignored.

Use this command to set the distance for an entire group of routes, rather than a specific route that passes an access list.

Examples To set the following administrative distances for route types in OSPF 100:

- 20 for inter-area routes

- 10 for intra-area routes
- 40 for external routes

use the commands:

```
awplus(config)# router ipv6 ospf 100
awplus(config-router)# distance ospfv3 inter-area 20 intra-area
10 external 40
```

To set the administrative distance for all routes in OSPFv3 100 back to the default of 110, use the commands:

```
awplus(config)# router ipv6 ospf 100
awplus(config-router)# no distance ospfv3
```

distribute-list (IPv6 OSPF)

Overview Use this command to apply filtering to the transfer of routing information between OSPFv3 and the IPv6 route table.

The entities that are used to perform filtering are ACLs (Access Control Lists), which match on certain attributes in the routes that are being transferred. For information about ACLs, see the ACL Feature Overview and Configuration Guide.

Use the **no** variant of this command to disable this feature for networks as defined in an associated access-list.

Syntax

```
distribute-list <access-list> in
no distribute-list [<access-list>] in
distribute-list <access-list> out {connected|ospf
[<process-tag>]|rip|static}
no distribute-list <access-list> out {connected|ospf
[<process-tag>]|rip|static}
```

Parameter	Description
<access-list>	Specifies the IPv6 access-list number or name to use. The specified access list defines which networks are received and which are suppressed.
`in`	Indicates that this applies to incoming advertised routes.
`out`	Indicates that this applies to outgoing advertised routes.
`connected`	Specify the redistribution of connected routes.
`ospf`	Specify the redistribution of OSPFv3 routes.
<process-tag>	Optionally specify an OSPFv3 process tag for OSPFv3 routes.
`rip`	Specify the redistribution of RIPng routes.
`static`	Specify the redistribution of connected routes.

Default Disabled

Mode Router Configuration

Usage notes This command applies filtering to the transfer of routing information between OSPFv3 and the IPv6 route table. You can apply filtering in either direction, from OSPFv3 to the IPv6 route table using an **in** distribute-list, or from the IPv6 route table to OSPFv3 using an **out** distribute-list.

The effect of an **in** filter is that some route information that OSPFv3 has learned from LSA updates will not be installed into the IPv6 route table. The effect of an **out** filter is that some route information that could be redistributed to OSPFv3 will not be redistributed to OSPFv3.

There are **in** and **out** distribute-lists, which carry out different route filtering activities:

- The **in** distribute list is applied to the process of installing OSPFv3 routes into the IPv6 route table. The SPF calculation generate a set of routes calculated from the LSA database. By default, all of these routes become OSPFv3 candidate routes for inclusion into the IPv6 route table.
- An **in** distribute-list can be used to control whether or not certain routes generated by the SPF calculation are included into the set of candidates for inclusion into the IP route table. Those routes that match **deny** entries in the distribute-list will not be considered for inclusion into the IPv6 route table.
- The **out** distribute-list applies the process of redistributing non-OSPFv3 routes into OSPFv3. If OSPFv3 redistribution is configured, and an **out** distribute-list is also configured, then routes that match deny entries in the distribute-list will not be redistributed into OSPFv3.

Example The below commands redistribute incoming route updates from networks defined with the standard named access-list called `myacl`:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard myacl permit
2001:db8:1::/64
awplus(config)# router ipv6 ospf
awplus(config-router)# distribute-list myacl in
```

The below commands redistribute outgoing connected route updates from networks defined with the standard named access-list called `myacl`:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard myacl permit
2001:db8:1::/64
awplus(config)# router ipv6 ospf
awplus(config-router)# distribute-list myacl out connected
```

The below commands disable incoming route updates from networks defined with the standard named access-list called `myacl`:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no distribute-list myacl in
```

The below commands disable outgoing connected route updates from networks defined with the standard named access-list called `myacl`:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no distribute-list myacl out connected
```

Related commands

ipv6 access-list extended (named)

ipv6 access-list standard (named)

ipv6 ospf authentication spi

Overview Use this command in Interface Configuration mode to enable either MD5 (Message-Digest 5) or SHA1 (Secure Hash Algorithm 1) authentication for a specified interface.

Use the **no** variant of this command in Interface Configuration mode to disable the authentication configured for a specified interface.

Syntax

```
ipv6 ospf authentication ipsec spi <256-4294967295> {md5 <MD5-key>|sha1 <SHA1-key>}
ipv6 ospf authentication null
no ipv6 ospf authentication ipsec spi <256-4294967295>
```

Parameter	Description
`authentication`	Specify this keyword to enable authentication.
`ipsec`	Specify this keyword to use IPsec authentication.
`spi`	Specify this keyword to set the SPI (Security Parameters Index).
`<256-4294967295>`	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.
`md5`	Specify the MD5 (Message-Digest 5) hashing algorithm.
`<MD5-key>`	Enter an MD5 key containing up to 32 hexadecimal characters.
`sha1`	Specify the SHA-1 (Secure Hash Algorithm 1) hashing algorithm.
`<SHA1-key>`	Enter an SHA-1 key containing up to 40 hexadecimal characters.
`null`	Specify no authentication is applied when no other parameters are applied after this keyword (`ipv6 ospf authentication null`). Note this overrides any existing area authentication configured.

Mode Interface Configuration

Default Authentication is not configured on an interface by default.

Usage notes Configure the same SPI (Security Parameters Index) value on all interfaces that connect to the same link. SPI values are used by link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

Use the **null** keyword to override existing area authentication. Apply the **null** keyword if area authentication is already configured to configure authentication on an interface.

See the OSPFv3 Feature Overview and Configuration Guide for more information and examples.

NOTE: *You can configure an authentication security policy (SPI) on a VLAN interface with this command, or an OSPFv3 area with the area authentication ipsec spi command.*

When you configure authentication for an area, the security policy is applied to all VLAN interfaces in the area. Allied Telesis recommends a different authentication security policy is applied to each interface for higher security.

If you apply the ***ipv6 ospf authentication null*** *command, this affects authentication configured on both the VLAN interface and the OSPFv3 area.*

This is due to OSPFv3 hello messages ingressing VLAN interfaces, which are part of area authentication, not being authenticated. So neighbors time out.

Example To enable MD5 authentication with a 32 hexadecimal character key for interface VLAN 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# area 1 authentication ipsec spi 1000 md5
1234567890ABCDEF1234567890ABCDEF
```

To enable SHA-1 authentication with a 40 hexadecimal character key for interface VLAN 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf authentication ipsec spi 1000 sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To specify no authentication is applied to interface VLAN 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf authentication null
```

To disable authentication for interface VLAN 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 ospf authentication ipsec spi 1000
```

Related commands

area authentication ipsec spi

area encryption ipsec spi esp

ipv6 ospf encryption spi esp

show ipv6 ospf interface

ipv6 ospf cost

Overview This command explicitly specifies the cost of the link-state metric in a router-LSA.

The interface cost indicates the overhead required to send packets across a certain VLAN interface. Use this command to set the VLAN interface cost manually.

The **no** variant of this command resets the VLAN interface cost to the default.

Syntax

```
ipv6 ospf cost <1-65535>
no ipv6 ospf cost
```

Parameter	Description
<1-65535>	The link-state metric.

Default By default there is no static value set and the OSPF cost is automatically calculated by using the command auto-cost reference bandwidth (IPv6 OSPF).

Mode Interface Configuration for a VLAN interface.

Usage notes This command explicitly sets a user specified cost of sending packets out the interface. Using this command overrides the cost value calculated automatically with the auto-cost reference bandwidth (IPv6 OSPF) feature.

The link-state metric cost is stated in the Router-LSA's link. Typically, the cost is inversely proportional to the bandwidth of an interface. By default, the cost of a VLAN interface is calculated according to the following formula:

reference bandwidth / interface bandwidth

The reference bandwidth is set by default at 1000000 kbps (or 1000 Mbps), but can be changed by the command auto-cost reference bandwidth (IPv6 OSPF).

The interface bandwidth is set by default to 1000000 kbps (or 1000 Mbps), but can be changed by the bandwidth command.

Example To set the IPv6 OSPF cost to 10 on the VLAN interface `vlan25`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan25
awplus(config-if)# ipv6 ospf cost 10
```

Related commands

show ipv6 ospf interface

auto-cost reference bandwidth (IPv6 OSPF)

bandwidth

ipv6 ospf dead-interval

Overview This command sets the interval during which no hello packets are received and after which a neighbor is declared dead.

The dead-interval is the amount of time that OSPF waits to receive an OSPF hello packet from the neighbor before declaring the neighbor is down. This value is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

The **no** variant of this command returns the interval to the default of 40 seconds.

Syntax

```
ipv6 ospf dead-interval <1-65535> [<inst-id>]
no ipv6 ospf  dead-interval
```

Parameter	Description
<1-65535>	The interval in seconds. Default: `40`
<inst-id>	The instance ID Default: `0`

Mode Interface Configuration for a VLAN interface.

Example The following example shows configuring the dead-interval to 10 seconds on the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf dead-interval 10
```

Related commands ipv6 ospf hello-interval

show ipv6 ospf interface

ipv6 ospf display route single-line

Overview Use this command to change the result of the **show ipv6 route** command to display each route entry on a single line.

Syntax

```
ipv6 ospf display route single-line
no ipv6 ospf display route single-line
```

Mode Global Configuration

Example To display each route entry on a single line.

```
awplus# configure terminal
awplus(config)# ipv6 ospf display route single-line
```

Related commands show ipv6 ospf route

ipv6 ospf encryption spi esp

Overview Use this command in Interface Configuration mode to enable either AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) or 3DES (Triple Data Encryption Standard) ESP (Encapsulating Security Payload) encryption for a specified interface.

Use the **no** variant of this command in Interface Configuration mode to disable the encryption configured for a specified interface.

Syntax

```
ipv6 ospf encryption ipsec spi <256-4294967295> esp {aes-cbc
<AES-CBC-key>|3des <3DES-key>|null}{md5 <MD5-key>|sha1
<SHA1-key>}
```

```
ipv6 ospf encryption null
```

```
no ipv6 ospf encryption ipsec spi <256-4294967295>
```

Parameter	Description
<256-4294967295>	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.
`esp`	Specify the esp keyword (Encapsulating Security Payload) to then apply either AES-CBC or 3DES encryption.
`aes-cbc`	Specify this keyword to enable AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) encryption.
<AES-CBC-key>	Enter an AES-CBC key containing either 32, 48, or 64 hexadecimal characters.
`3des`	Specify 3DES (Triple Data Encryption Standard) encryption.
<3DES-key>	Enter a 3DES key containing 48 hexadecimal characters.
`null`	Specify ESP without AES-CBC or 3DES encryption applied.
`md5`	Specify the MD5 (Message-Digest 5) encryption algorithm.
<MD5-key>	Enter an MD5 key containing 32 hexadecimal characters.
`sha1`	Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.
<SHA1-key>	Enter an SHA-1 key containing 40 hexadecimal characters.
`null`	Specify no encryption is applied when no other parameters are applied after this keyword (`ipv6 ospf encryption null`).

Default Authentication is not configured on an interface by default.

Mode Interface Configuration

Usage notes When you issue this command, authentication and encryption are both enabled. Configure the same SPI (Security Parameters Index) value on all interfaces that connect to the same link. SPI values are used by link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

Security is achieved using the IPv6 ESP extension header. The IPv6 ESP extension header is used to provide confidentiality, integrity, authentication, and confidentiality. Authentication fields are removed from OSPF for IPv6 packet headers, so applying IPv6 ESP extension headers are required for integrity, authentication, and confidentiality.

Use the **null** keyword to override existing area encryption. Apply the **null** keyword if area encryption is already configured to then configure encryption on an interface instead.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

See the OSPFv3 Feature Overview and Configuration Guide for more information and examples.

NOTE: *You can configure an encryption security policy (SPI) on a VLAN interface with this command, or an OSPFv3 area with the area encryption ipsec spi esp command.*

When you configure encryption for an area, the security policy is applied to all VLAN interfaces in the area. Allied Telesis recommends a different encryption security policy is applied for each interface for higher security.

*If you apply the **ipv6 ospf encryption null** command this affects encryption configured on both the VLAN interface and the OSPFv3 area.*

This is due to OSPFv3 hello messages ingressing VLAN interfaces, which are part of area encryption, not being encrypted. So neighbors time out.

Example To enable ESP encryption, but not apply an AES-CBC key or a 3DES key, for interface VLAN 2 and MD5 authentication with a 32 hexadecimal character key, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf encryption ipsec spi 1000 esp null
md5 1234567890ABCDEF1234567890ABCDEF
```

To enable ESP encryption, but not apply an AES-CBC key or a 3DES key, for interface VLAN 2 and SHA-1 authentication with a 40 hexadecimal character key, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf encryption ipsec spi 1000 esp null
sha1 1234567890ABCDEF1234567890ABCDEF12345678
```

To enable ESP encryption with an 3DES key with a 48 hexadecimal character key and MD5 authentication with a 32 hexadecimal character key for interface VLAN 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf encryption ipsec spi 1000 esp 3des
1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF md5
1234567890ABCDEF1234567890ABCDEF
```

To enable ESP encryption with an AES-CBC key with a 32 hexadecimal character key and SHA-1 authentication with a 40 hexadecimal character key for interface VLAN 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf encryption ipsec spi 1000 esp
aes-cbc 1234567890ABCDEF1234567890ABCDEF sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To specify no ESP encryption is applied to interface VLAN 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf encryption null
```

To disable ESP encryption for interface VLAN 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 ospf encryption ipsec spi 1000
```

Related commands

area authentication ipsec spi

area encryption ipsec spi esp

ipv6 ospf authentication spi

show ipv6 ospf interface

ipv6 ospf hello-interval

Overview This command specifies the interval between hello packets.

The hello-interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter interval ensures faster detection of topological changes, but results in more routing traffic.

The **no** variant of this command returns the interval to the default of 10 seconds.

Syntax

```
ipv6 ospf hello-interval <1-65535>
no ipv6 ospf hello-interval
```

Parameter	Description
<1-65535>	The hello-interval in seconds. Default: `10`

Default The default interval is 10 seconds.

Mode Interface Configuration for a VLAN interface.

Example The following example shows setting the `hello-interval` to 3 seconds on the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf hello-interval 3
```

Related commands

ipv6 ospf dead-interval

show ipv6 ospf interface

ipv6 ospf neighbor

Overview Use this command to configure static OSPFv3 IPv6 neighbors when using the OSPFv3 "non-broadcast" (NBMA) and "point-to-multipoint non-broadcast" (P2MP NBMA) network types. OSPFv3 messages exchanged between the neighbors are unicast only.

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

Syntax

```
ipv6 ospf neighbor <ipv6-address>
[<cost>|<instance-id>|<poll-interval>|<priority>]

no ipv6 ospf neighbor <ipv6-address>
[<cost>|<instacne-id>|<poll-interval>|<priority>]
```

Parameter	Description
<ipv6-address>	Specifies the interface IPv6 address of the neighbor.
<cost>	*cost <1-65535>* OSPF cost for point-to-multipoint neighbor.
<instance-id>	*instance-id <0-255>* Interface instance ID.
<poll-interval>	*poll-interval <0-4294967295>* Dead neighbor polling interval in seconds. It is recommended to set this value much higher than the hello interval. The default is 120 seconds.
<priority>	*priority <0-255>* Specifies the router priority value of the non-broadcast neighbor associated with the specified IP address. The default is 0. This keyword does not apply to point-to-multipoint interfaces.

Mode Interface Configuration

Usage notes To configure a neighbor on an NBMA network manually, use the **ipv6 ospf neighbor** command and include one neighbor entry for each known non-broadcast network neighbor. The IPv6 address used in this command is the neighbor's primary IPv6 address on the interface where that neighbor connects to the NBMA network.

The poll interval is the reduced rate at which routers continue to send hello packets, when a neighboring router has become inactive. Set the poll interval to be much larger than hello interval.

You can use this command to configure static OSPFv3 IPv6 neighbors for Layer 3 interfaces, such as Ethernet or tunnel interfaces on routers or a VLAN interface on switches or routers.

Examples To configure a neighbor with a priority value, poll interval time, and cost, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf neighbor fe80::c:20:0:1 priority 1
poll-interval 90
awplus(config-router)# ipv6 ospf neighbor fe80::c:20:0:1 cost
15
```

Related commands show ipv6 ospf neighbor

ipv6 ospf network

Overview This command configures the OSPF network type to a type different from the default for the particular VLAN interface.

The **no** variant of this command returns the network type to the default for the particular VLAN interface.

Syntax

```
ipv6 ospf network [broadcast | non-broadcast | point-to-point |
point-to-multipoint]
```

```
no ipv6 ospf network
```

Parameter	Description
`broadcast`	Sets the network type to broadcast.
`non-broadcast`	Sets the network type to NBMA.
`point-to-multipoint`	Sets the network type to point-to-multipoint.
`point-to-point`	Sets the network type to point-to-point.

Default The default is the `broadcast` OSPF network type for a VLAN interface.

Mode Interface Configuration for a VLAN interface.

Usage notes This command forces the interface network type to the specified type. Depending on the network type, OSPF changes the behavior of the packet transmission and the link description in LSAs.

Example The following example shows setting the network type to `point-to-point` on the VLAN interface `vlan1`:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 ospf network point-to-point
```

ipv6 ospf priority

Overview This command sets the router priority, which is a parameter used in the election of the designated router for the link.

The **no** variant of this command returns the router priority to the default of 1.

Syntax

```
ipv6 ospf priority <priority>
no ipv6 ospf priority
```

Parameter	Description
<priority>	*<0-255>* Specifies the router priority of the interface. The larger the value, the greater the priority level. The value 0 defines that the device cannot become either the DR, or backup DR for the link.

Default The default priority is 1.

Mode Interface Configuration for a VLAN interface.

Usage Set the priority to help determine the OSPF Designated Router (DR) for a link. If two routers attempt to become the DR, the router with the higher router priority becomes the DR. If the router priority is the same for two routers, the router with the higher router ID takes precedence.

Routers with zero router priority values cannot become the designated or backup designated router.

Example The following example shows setting the OSPFv3 priority value to 3 on the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf priority 3
```

ipv6 ospf retransmit-interval

Overview Use this command to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.

Use the **no** variant of this command to return to the default of 5 seconds.

Syntax

```
ipv6 ospf retransmit-interval <1-65535>
no ipv6 ospf retransmit-interval
```

Parameter	Description
<1-65535>	Specifies the interval in seconds.

Default The default interval is 5 seconds.

Mode Interface Configuration for a VLAN interface.

Usage After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgment. In case the router does not receive an acknowledgment during the set time (the retransmit interval value) it retransmits the LSA. Set the retransmission interval value conservatively to avoid needless retransmission. The interval should be greater than the expected round-trip delay between two routers.

Example The following example shows setting the `ospf retransmit interval` to 6 seconds on the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf retransmit-interval 6
```

ipv6 ospf transmit-delay

Overview Use this command to set the estimated time it takes to transmit a link-state-update packet on the VLAN interface.

Use the **no** variant of this command to return to the default of 1 second.

Syntax

```
ipv6 ospf transmit-delay <1-65535>
no ipv6 ospf transmit-delay
```

Parameter	Description
<1-65535>	Specifies the time, in seconds, to transmit a link-state update.

Default The default interval is 1 second.

Mode Interface Configuration for a VLAN interface.

Usage The transmit delay value adds a specified time to the age field of an update. If the delay is not added, the time in which the LSA transmits over the link is not considered. This command is especially useful for low speed links. Add transmission and propagation delays when setting the transmit delay value.

Example To set the IPv6 OSPF transmit delay time to 3 seconds on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 ospf transmit-delay 3
```

ipv6 router ospf area

Overview Use this command to enable IPv6 OSPF routing on an interface.

Use the **no** variant of this command to disable IPv6 OSPF routing on an interface.

Syntax

```
ipv6 router ospf area <area-id> [tag <process-id>] [instance <inst-id>]
no ipv6 router ospf area <area-id>
```

Parameter	Description
<area-id>	The ID of the IPv6 OSPF routing area. Can be entered as either an IPv4 A.B.C.D address format, or as an unsigned integer in the range, 0 to 4294967295. Use either of the following forms when entering an area-ID: • `area-id` *<A.B.C.D>* where A.B.C.D is a number entered in IPv4 address format. • `area-id` <0 to 4294967295>.
<process-id>	The process tag denotes a separate router process. It can comprise any string of alphanumeric characters. Note that this tag is local to the router on which it is set and does not appear in any OSPF packets or LSA.
<instance-id>	The OSPF instance ID, entered as an integer between 0 and 255. This is the value that will appear in the instance field of the IPv6 OSPF hello packet.

Defaults IPv6 OSPF routing is disabled by default.

When enabling IPv6 OSPF routing:

- the process-tag will default to a null value if not set.
- the Instance ID defaults to 0 if not set.

Mode Interface Configuration for a VLAN interface.

Usage notes When enabling IPv6 OSPF routing on an interface, specifying the area-ID is mandatory, but the Process tag and Instance are optional.

See the OSPFv3 Feature Overview and Configuration Guide for more information and examples.

Examples The following commands enable IPv6 OSPF on VLAN interface `vlan2`, OSPF area 1, tag PT2, and instance 2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 router ospf area 1 tag PT2 instance-id 2
```

The following commands disable IPv6 OSPF on VLAN interface `vlan2` and OSPF area 1:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 router ospf area 1
```

max-concurrent-dd (IPv6 OSPF)

Overview Use this command to limit the number of neighbors that can be concurrently processed in the database exchange. The specified value limits the number of neighbors from all interfaces, not per interface.

Use the **no** variant of this command to have no limit on the maximum number of LSAs.

Syntax

```
max-concurrent-dd <max-neighbors>
no max-concurrent-dd
```

Parameter	Description
<max-neighbors>	<1-65535> The maximum number of neighbors.

Mode Router Configuration

Usage notes This command is useful where bringing up several adjacencies on a router is affecting performance. In this situation, you can often enhance the system performance by limiting the number of neighbors that can be processed concurrently.

Example The following example sets the max-concurrent-dd value to allow only 4 neighbors to be processed at a time.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# max-concurrent-dd 4
```

Related commands router ipv6 ospf

passive-interface (IPv6 OSPF)

Overview Use this command to suppress the sending of Hello packets on a specified interface. If you use the **passive-interface** command without the optional parameters then **all** interfaces are put into passive mode.

Use the **no** variant of this command to allow the sending of Hello packets on all interfaces, or on the specified interface. If you use the **no** variant of this command without the optional parameters then **all** interfaces are removed from passive mode.

Syntax

```
passive-interface [<interface>]
no passive-interface [<interface>]
```

Parameter	Description
<interface>	The name or the VID of the VLAN interface.

Mode Router Configuration

Usage Configure an interface to be passive if you wish its connected route to be treated as an OSPF route (rather than an AS-external route), but do not wish to actually exchange any OSPF packets via this interface.

Examples To configure passive interface mode on interface vlan2, enter the following commands:

```
awplus(config)# router ipv6 ospf
awplus(config-router)# passive-interface vlan2
```

To configure passive interface mode on **all** interfaces, enter the following commands:

```
awplus(config)# router ipv6 ospf
awplus(config-router)# passive-interface
```

To remove passive interface mode on interface vlan2, enter the following commands:

```
awplus(config)# router ipv6 ospf
awplus(config-router)# no passive-interface vlan2
```

To remove passive interface mode on **all** interfaces, enter the following commands:

```
awplus(config)# router ipv6 ospf
awplus(config-router)# no passive-interface
```

redistribute (IPv6 OSPF)

Overview Use this command to redistribute routes from other routing protocols, static routes and connected routes into an IPv6 OSPF routing table.

Use the **no** variant of this command to disable this function.

Syntax

```
redistribute <protocol>} [metric <0-16777214>] [metric-type
{1|2}] [route-map <route-map-entry>]
no redistribute <protocol>
```

Parameter	Description	
<protocol>	The routing protocol to be redistributed, can be one of:	
	`connected`	Connected routes
	`rip`	Routing Internet Protocol
	`static`	Static Routes
`metric`	Specifies the external metric.	
`metric-type`	Specifies the external metric-type, either type 1 or type 2. • **For Metric Type 1:** The best route is based on the external redistributed path cost plus the internal path cost presented by the native routing protocol. • **For Metric Type 2:** The best route is based only on the external redistributed path cost. The internal path cost is only used to break a "tie" situation between two identical external path costs.	
`route-map`	The name of the specific route-map.	

Default The default metric value for routes redistributed into OSPFv3 is 20. The metric can also be defined using the set metric command for a route map. Note that a metric defined using the set metric command for a route map overrides a metric defined with this command.

Mode Router Configuration

Usage notes You use this command to inject routes, learned from other routing protocols, into the OSPF domain to generate AS-external-LSAs. If a route-map is configured by this command, then that route-map is used to control which routes are redistributed and can set metric and tag values on particular routes.

The metric, metric-type, and tag values specified on this command are applied to any redistributed routes that are not explicitly given a different metric, metric-type, or tag value by the route map.

See the OSPFv3 Feature Overview and Configuration Guide for more information about metrics, and about behavior when configured in route maps.

Note that this command does not redistribute the default route. To redistribute the default route, use the default-information originate command.

Example The following example shows the redistribution of RIP routes into the IPv6 OSPF routing table, with a metric of 10 and a metric type of 1.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# redistribute rip metric 10 metric-type 1
```

restart ipv6 ospf graceful

Overview Use this command to force the OSPFv3 process to restart. You may optionally specify a grace-period value. If a grace-period is not specified then a default value of 120 seconds is applied.

You should specify a grace-period value of 120 seconds or more. Low grace-period values may cause the graceful restart process on neighboring routers to terminate with routes missing.

Syntax

```
restart ipv6 ospf graceful [grace-period <1-1800>]
```

Parameter	Description
`grace-period`	Specify the grace period.
<1-1800>	The grace period in seconds.

Default The default OSPF grace-period is 120 seconds.

Mode Privileged Exec

Usage notes After this command is executed, the OSPFv3 process immediately shuts down. It notifies the system that OSPF has performed a graceful shutdown. Routes installed by OSPF are preserved until the grace-period expires.

When a **restart ospf graceful** command is issued, the OSPF configuration is reloaded from the last saved configuration. Ensure you first enter the copy running-config startup- config command.

Example To restart OSPFv3, use the following commands:

```
awplus# copy running-config startup-config
awplus# restart ipv6 ospf graceful grace-period 200
```

To apply the default grace-period (120 seconds), use the following commands:

```
awplus# copy running-config startup-config
awplus# restart ipv6 ospf graceful
```

router ipv6 ospf

Overview Use this command to create or remove an IPv6 OSPF routing process, or to enter the Router Configuration mode to configure a specific IPv6 OSPF routing process. Use the **no** variant of this command to terminate an IPv6 OSPF routing process.

Use the **no** parameter with the **process-id** parameter, to terminate and delete a specific IPv6 OSPF routing process.

Syntax

```
router ipv6 ospf [<process-id>]
no router ipv6 ospf [<process-id>]
```

Parameter	Description
<process-id>	A character string that identifies a routing process. If you do not specify the process-id a "null" process ID will be applied. Note that this will appear in show output as *null* However you cannot select the null process by using the character string *null* as command entry characters.

Default No routing process is defined by default.

Mode Global Configuration

Usage notes The process ID enables you to run more than one OSPF session within the same router, then configure each session to a different router port. Note that this function is internal to the router, and other routers (neighbors) have no knowledge of these different processes. The hello and LSAs issued from each process will appear as if coming from a separate physical router.

To a large extent the requirement for multiple processes has been replaced by the ability within IPv6 OSPF of running simultaneous router instances.

The process ID of IPv6 OSPF is an optional parameter for the **no** variant of this command only. When removing all IPv6 OSPF processes on the device, you do not need to specify each Process ID, but when removing particular IPv6 OSPF processes, you must specify each Process ID to be removed.

For a description of processes and instances and their configuration relationships, see the OSPFv3 Feature Overview and Configuration Guide.

Example This example shows the use of this command to enter Router Configuration mode.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf P100
awplus(config-router)#
```

router-id (IPv6 OSPF)

Overview Use this command to specify a router ID for the IPv6 OSPF process.

Use the **no** variant of this command to disable this function.

Syntax

```
router-id <router-id>
no router-id
```

Parameter	Description
<router-id>	Specifies the router ID in IPv4 address format.

Mode Router Configuration

Usage Configure each router with a unique router-id. In an IPv6 OSPF router process that has active neighbors, a new router-id takes effect at the next reload or when you restart OSPF manually.

Example The following example shows a specified router ID 0.0.4.5.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# router-id 0.0.4.5
```

Related commands show ipv6 ospf

show debugging ipv6 ospf

Overview Use this command to see what debugging is turned on for OSPFv3.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show debugging ipv6 ospf
```

Mode User Exec and Privileged Exec

Example

```
awplus# show debugging ipv6 ospf
```

Output Figure 29-1: Example output from the **show debugging ipv6 ospf** command

```
OSPFv3 debugging status:
  OSPFv3 all packet detail debugging is on
  OSPFv3 all IFSM debugging is on
  OSPFv3 all NFSM debugging is on
  OSPFv3 all LSA debugging is on
  OSPFv3 all NSM debugging is on
  OSPFv3 all route calculation debugging is on
  OSPFv3 all event debugging is on
```

show ipv6 ospf

Overview Use this command in User Exec or Privileged Exec modes to display general information about all IPv6 OSPF routing processes, including OSPFv3 Authentication configuration and status information.

Include the process ID parameter with this command to display information about specified processes.

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

Syntax

```
show ipv6 ospf
show ipv6 ospf <process-id>
```

Parameter	Description
<process-id>	*<0-65535>* The ID of the router process for which information will be displayed. If this parameter is included, only the information for the specified routing process is displayed.

Mode User Exec and Privileged Exec

Examples To display general information about all IPv6 OSPF routing processes, use the command:

```
awplus# show ipv6 ospf
```

To display general information about IPv6 OSPF (OSPFv3) routing process `P10`, use the command:

```
awplus# show ipv6 ospf P10
```

Output Figure 29-2: Example output from the **show ipv6 ospf** command for process P10, showing OSPFv3 Authentication configuration information highlighted in bold

```
 awplus#show ipv6 ospf
  Routing Process "OSPFv3 (10)" with ID 192.168.1.2
  Route Licence: Route : Limit=Unlimited, Allocated=0, Visible=0,
Internal=0
  Route Licence: Breach: Current=0, Watermark=0
  Process uptime is 6 minutes
  Current grace period is 120 secs (default)
  SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0
secs
  Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
  Number of incoming current DD exchange neighbors 0/5
  Number of outgoing current DD exchange neighbors 0/5
  Number of external LSA 0. Checksum Sum 0x0000
  Number of AS-Scoped Unknown LSA 0
  Number of LSA originated 4
  Number of LSA received 10
  Number of areas in this router is 1
     Area BACKBONE(0)
         Number of interfaces in this area is 1(1)
         MD5 Authentication SPI 1000
         NULL Encryption SHA-1 Auth, SPI 1001
         SPF algorithm executed 9 times
         Number of LSA 3.  Checksum Sum 0xF9CC
         Number of Unknown LSA 0
```

Related commands

area authentication ipsec spi

area encryption ipsec spi esp

router ipv6 ospf

show ipv6 ospf database

Overview Use this command in User Exec or Privileged Exec modes to display a database summary for IPv6 OSPF information. Include the process ID parameter with this command to display information about specified processes.

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

Syntax

```
show ipv6 ospf <process-id> database
[self-originate|max-age|adv router <adv-router-id>]
```

Parameter	Description
<process-id>	*<0-65535>* The ID of the router process for which information will be displayed.
`self-originate`	Displays self-originated link states.
`max-age`	Displays LSAs in MaxAge list. It maintains the list of the all LSAs in the database which have reached the max-age which is 3600 seconds.
`adv-router`	Advertising Router LSA.
<adv-router- id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.

Mode User Exec and Privileged Exec

Example To display the database summary for IPv6 OSPF information on process `P10`, use the command:

```
awplus# show ipv6 ospf P10 database
```

Output Figure 29-3: Example output from the **show ipv6 ospf P10 database** command

```
OSPFv3 Router with ID (0.0.1.1) (Process P10)

                Link-LSA (Interface vlan2)

Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.0.202       0.0.1.1           46 0x800000c3 0x5f50      1
0.0.0.202       0.0.1.2            8 0x800000c3 0x4ca0      1

                Link-LSA (Interface vlan3)

Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.0.203       0.0.1.1         1071 0x8000000e 0xe082      1
0.0.0.203       0.0.1.3         1057 0x8000000e 0xb8aa      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age  Seq#       CkSum    Link
0.0.0.0         0.0.1.1         1016 0x800000cd 0xa426      2
0.0.0.0         0.0.1.2          979 0x800000d8 0xad2b      1
0.0.0.0         0.0.1.3         1005 0x800000cf 0xefed      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age  Seq#       CkSum
0.0.0.202       0.0.1.2         1764 0x800000c2 0x94c3
0.0.0.203       0.0.1.3         1010 0x800000c4 0x8ac8

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age  Seq#       CkSum  Prefix  Reference
0.0.0.2         0.0.1.2          978 0x800000a1 0x699a      1  Router-LSA
0.0.0.4         0.0.1.2         1764 0x800000c2 0xca4d      1  Network-LSA
0.0.0.1         0.0.1.3         1004 0x80000012 0xaee2      1  Router-LSA
0.0.0.7         0.0.1.3         1005 0x8000000e 0x3c89      1  Network-LSA

                AS-external-LSA

Link State ID   ADV Router      Age  Seq#       CkSum
0.0.0.13        0.0.1.1         1071 0x8000000e 0xca9f E2
0.0.0.14        0.0.1.1         1071 0x8000000e 0xcc9b E2
0.0.0.15        0.0.1.1         1071 0x8000000e 0xce97 E2
0.0.0.16        0.0.1.1         1071 0x8000000e 0xd093 E2
0.0.0.17        0.0.1.1         1071 0x8000000e 0xd28f E2
0.0.0.18        0.0.1.1         1071 0x8000000e 0xd48b E2
```

show ipv6 ospf database external

Overview Use this command in User Exec or Privileged Exec modes to display information about the external LSAs.

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

Syntax

```
show ipv6 ospf database external <adv-router-id>
[self-originate|adv-router <adv-router-id>]
```

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
`self-originate`	Self-originated link states.
`adv-router`	Displays all the LSAs of the specified router.

Mode User Exec and Privileged Exec

Examples To display information about the external LSAs, use the following command:

```
awplus# show ipv6 ospf database external adv-router 10.10.10.1
```

Output Figure 29-4: Example output from the **show ipv6 ospf database external** command

```
LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.13
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xCE9D
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2010:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
...
```

show ipv6 ospf database grace

Overview Use this command in User Exec or Privileged Exec modes to display information about the grace LSAs.

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

Syntax

```
show ipv6 ospf database grace <adv-router-id>
[self-originate|adv-router <adv-router-id>]
```

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
adv-router	Displays all the LSAs of the specified router.
self-originate	Self-originated link states.

Mode User Exec and Privileged Exec

Examples To display information about the grace LSAs, use the following command:

```
awplus# show ipv6 ospf database grace adv-router 10.10.10.1
```

Output Figure 29-5: Example output from the **show ipv6 ospf database grace** command

```
LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.13
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xCE9D
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2010:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
```

show ipv6 ospf database inter-prefix

Overview Use this command in User Exec or Privileged Exec modes to display information about the inter-prefix LSAs.

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

Syntax

```
show ipv6 ospf database inter-prefix <adv-router-id>
[self-originate|adv-router <adv-router-id>]
```

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
`adv-router`	Displays all the LSAs of the specified router.
`self-originate`	Self-originated link states.

Mode User Exec and Privileged Exec

Examples To display information about the inter-prefix LSAs, use the following command:

```
awplus# show ipv6 ospf database external adv-router 10.10.10.1
```

Output Figure 29-6: Example output from the **show ipv6 ospf database inter-prefix** command

```
LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.13
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xCE9D
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2010:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
...
```

show ipv6 ospf database inter-router

Overview Use this command in User Exec or Privileged Exec modes to display information about the inter-router LSAs.

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

Syntax

```
show ipv6 ospf database inter-router <adv-router-id>
[self-originate| adv-router <adv-router-id>]
```

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
adv-router	Displays all the LSAs of the specified router.
self-originate	Self-originated link states.

Mode User Exec and Privileged Exec

Examples To display information about the inter-router LSAs, use the following command:

```
awplus# show ipv6 ospf database inter-router adv-router
10.10.10.1
```

Output Figure 29-7: Example output from the **show ipv6 ospf database inter-router** command

```
LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.13
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xCE9D
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2010:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
...
```

show ipv6 ospf database intra-prefix

Overview Use this command in User Exec or Privileged Exec modes to display information about the intra-prefix LSAs.

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

Syntax

```
show ipv6 ospf database intra-prefix <adv-router-id>
[self-originate|adv-router <adv-router-id>]
```

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
adv-router	Displays all the LSAs of the specified router.
self-originate	Self-originated link states.

Mode User Exec and Privileged Exec

Examples To display information about the intra-prefix LSAs, use the following command:

```
awplus# show ipv6 ospf database intra-prefix adv-router
10.10.10.1
```

Output Figure 29-8: Example output from the **show ipv6 ospf database intra-prefix** command

```
LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.13
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xCE9D
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2010:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
...
```

show ipv6 ospf database link

Overview Use this command in User Exec or Privileged Exec modes to display information about the link LSAs.

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

Syntax

```
show ipv6 ospf database link <adv-router-id>
[self-originate|adv-router <adv-router-id>]
```

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
`adv-router`	Displays all the LSAs of the specified router.
`self-originate`	Self-originated link states.

Mode User Exec and Privileged Exec

Examples To display information about the link LSAs, use the following command:

```
awplus# show ipv6 ospf database link adv-router 10.10.10.1
```

Output Figure 29-9: Example output from the s**how ipv6 ospf database link** command

```
LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.13
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xCE9D
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2010:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
...
```

show ipv6 ospf database network

Overview Use this command in User Exec or Privileged Exec modes to display information about the network LSAs.

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

Syntax

```
show ipv6 ospf database network <adv-router-id>
[self-originate|adv-router <adv-router-id>]
```

Parameter	Description
<adv-router-id>	The router ID of the advertising router, in IPv4 address format. Note, however, that this no longer represents a real address.
`self-originate`	Self-originated link states.
`adv-router`	The advertising router selected.

Mode User Exec and Privileged Exec

Examples To display information about the OSPFv3 network LSAs, use the following command:

```
awplus# show ipv6 ospf database network
```

Output Figure 29-10: Example output from the **show ipv6 ospf database network** command

```
OSPFv3 Router with ID (0.0.1.1) (Process P10)

                Network-LSA (Area 0.0.0.0)

  LS age: 97
  LS Type: Network-LSA
  Link State ID: 0.0.0.202
  Advertising Router: 0.0.1.2
  LS Seq Number: 0x800000C3
  Checksum: 0x92C4
  Length: 32
  Options: 0x000013 (-|R|-|-|E|V6)
    Attached Router: 0.0.1.2
    Attached Router: 0.0.1.1
```

```
  LS age: 1144
  LS Type: Network-LSA
  Link State ID: 0.0.0.203
  Advertising Router: 0.0.1.3
  LS Seq Number: 0x800000C4
  Checksum: 0x8AC8
  Length: 32
  Options: 0x000013 (-|R|-|-|E|V6)
    Attached Router: 0.0.1.3
    Attached Router: 0.0.1.1
```

show ipv6 ospf database router

Overview Use this command in User Exec or Privileged Exec modes to display information only about the router LSAs.

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

Syntax

```
show ipv6 ospf database router <adv-router-id>
[self-originate|adv-router <adv-router-id>]
```

Parameter	Description
<adv-router-id>	The router ID of the advertising router, in IPv4 address format. Note, however, that this no longer represents a real address.
`self-originate`	Self-originated link states.
`adv-router`	The advertising router selected.

Mode User Exec and Privileged Exec

Examples To display information about the OSPFv3 router LSAs, use the following command:

```
awplus# show ipv6 ospf database router
```

Output Figure 29-11: Example output from the **show ipv6 ospf database router** command

```
           OSPFv3 Router with ID (0.0.1.3) (Process P10)

                Router-LSA (Area 0.0.0.0)

LS age: 556
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x800000CA
  Checksum: 0xAA23
  Length: 56
  Flags: 0x02 (-|-|E|-)
  Options: 0x000013 (-|R|-|-|E|V6)
```

```
    Link connected to: a Transit Network
      Metric: 1
      Interface ID: 203
      Neighbor Interface ID: 203
      Neighbor Router ID: 0.0.1.3

    Link connected to: a Transit Network
      Metric: 1
      Interface ID: 202
      Neighbor Interface ID: 202
      Neighbor Router ID: 0.0.1.2

  LS age: 520
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 0.0.1.2
  LS Seq Number: 0x800000D5
  Checksum: 0xB328
  Length: 40
  Flags: 0x00 (-|-|-|-)
  Options: 0x000013 (-|R|-|-|E|V6)

    Link connected to: a Transit Network
      Metric: 1
      Interface ID: 202
      Neighbor Interface ID: 202
      Neighbor Router ID: 0.0.1.2

LS age: 543
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 0.0.1.3
  LS Seq Number: 0x800000CC
  Checksum: 0xF5EA
  Length: 40
  Flags: 0x00 (-|-|-|-)
  Options: 0x000013 (-|R|-|-|E|V6)

    Link connected to: a Transit Network
      Metric: 1
      Interface ID: 203
      Neighbor Interface ID: 203
      Neighbor Router ID: 0.0.1.3
            OSPFv3 Router with ID (0.0.1.3) (Process P10)

                AS-external-LSA
```

```
  LS age: 1384
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.13
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x80000009
  Checksum: 0xD49A
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2010:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1384
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.14
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x80000009
  Checksum: 0xD696
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2011:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1384
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.15
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x80000009
  Checksum: 0xD892
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2012:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.13
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xCE9D
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2010:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
```

```
LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.14
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xD099
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2011:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.15
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xD295
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2012:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.16
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xD491
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2013:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.17
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xD68D
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2014:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
```

```
LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.18
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xD889
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2015:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
```

show ipv6 ospf interface

Overview Use this command in User Exec or Privileged Exec modes to display interface information for OSPF for all interfaces or a specified interface, including OSPFv3 Authentication status for all interfaces or for a specified interface.

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

Syntax

```
show ipv6 ospf interface [<interface-name>]
```

Parameter	Description
<interface-name>	An alphanumeric string that is the interface name. Omit the optional interface to display OSPF

Mode User Exec and Privileged Exec

Examples

```
awplus# show ipv6 ospf interface vlan2
```

Output Figure 29-12: Example output from the **show ipv6 ospf interface** command showing OSPFv3 Authentication configuration information highlighted in bold

```
awplus#show ipv6 ospf interface
 vlan2 is up, line protocol is up
   Interface ID 302
   IPv6 Prefixes
     fe80::215:77ff:fead:f87e/64 (Link-Local Address)
   Security Policy
     MD5 Authentication SPI 1000
     NULL Encryption SHA-1 Auth, SPI 1001

   OSPFv3 Process (10), Area 0.0.0.0, Instance ID 0
     Router ID 192.168.1.2, Network Type BROADCAST, Cost: 1
     Transmit Delay is 1 sec, State Backup, Priority 1
     Interface state Backup
     Designated Router (ID) 192.168.1.1
       Interface Address fe80::21d:e5ff:fec9:cfbe
     Backup Designated Router (ID) 192.168.1.2
       Interface Address fe80::215:77ff:fead:f87e
     Timer interval configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
       Hello due in 00:00:07
     Neighbor Count is 1, Adjacent neighbor count is 1
```

Figure 29-13: Example output from the **show ipv6 ospf interface** vlan3 command

```
awplus#show ipv6 ospf interface vlan3
vlan3 is up, line protocol is up
  Interface ID 203
  IPv6 Prefixes
    fe80::200:cdff:fe24:daae/64 (Link-Local Address)
    2003:1111::2/64
  OSPFv3 Process (P1), Area 0.0.0.0, Instance ID 0
    Router ID 0.0.1.1, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 0.0.1.1
      Interface Address fe80::200:cdff:fe24:daae
    No backup designated router on this link
    Timer interval configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
      Hello due in 00:00:02
    Neighbor Count is 0, Adjacent neighbor count is 0
```

Related commands

ipv6 ospf authentication spi

ipv6 ospf encryption spi esp

show ipv6 ospf neighbor

Overview Use this command in User Exec or Privileged Exec modes to display information on OSPF neighbors. Include the process ID parameter with this command to display information about specified processes.

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

Syntax

```
show ipv6 ospf [<process-id>] neighbor <neighbor-id>
show ipv6 ospf [<process-id>] neighbor detail
show ipv6 ospf [<process-id>] neighbor <interface> [detail]
```

Parameter	Description
<process-id>	*<character string>* The ID of the OSPF process for which information will be displayed.
<neighbor-id>	The Neighbor ID, entered in IP address (A.B.C.D) format.
detail	Detail of all neighbors.
<interface>	IP address of the interface.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ipv6 ospf neighbor
```

Output Figure 29-14: Example output from **show ipv6 ospf neighbor**

```
awplus#show ipv6 ospf P1 neighbor 2.2.2.2
OSPFv3 Process (P1)
Neighbor ID     Pri      State                  Dead Time   Interface Instance ID
2.2.2.2         5        2-Way/DROther          00:00:33    vlan3              0
```

Figure 29-15: Example output from **show ipv6 ospf neighbor detail**

```
awplus#show ipv6 ospf neighbor detail
Neighbor 0.0.1.2, interface address fe80::215:77ff:fec9:7472
   In the area 0.0.0.0 via interface vlan2
   Neighbor priority is 1, State is Full, 6 state changes
   DR is 0.0.1.2     BDR is 0.0.1.1
   Options is 0x000013 (-|R|-|-|E|V6)
   Dead timer due in 00:00:33
   Database Summary List 0
   Link State Request List 0
   Link State Retransmission List 0
```

show ipv6 ospf route

Overview Use this command in User Exec or Privileged Exec modes to display the OSPF routing table. Include the process ID parameter with this command to display the OSPF routing table for specified processes.

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

Syntax

```
show ipv6 ospf [<process-id>] route
```

Parameter	Description
<process-id>	A character string that specifies the router process. If this parameter is included, only the information for this specified routing process is displayed.

Mode User Exec and Privileged Exec

Examples To display the OSPF routing table, use the command:

```
awplus# show ipv6 ospf route
```

Output Figure 29-16: Example output from the **show ipv6 ospf P10 route** command for a specific process

```
OSPFv3 Process (P1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter
area
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
O  2002:1111::/64                                    2
     via fe80::200:cdff:fe24:daae, vlan3, Area 0.0.0.0
C  2003:1111::/64                                    1
     directly connected, vlan3, Area 0.0.0.0
O  2004:1111::/64                                    3
     via fe80::200:cdff:fe24:daae, vlan3, Area 0.0.0.0
C  2005:1111::/64                                    1
     directly connected, vlan5, Area 0.0.0.0
E2 2010:2222::/64                                 1/20
     via 2003:1111::1, vlan3
E2 2011:2222::/64                                 1/20
     via 2003:1111::1, vlan3
E2 2012:2222::/64                                 1/20
     via 2003:1111::1, vlan3
E2 2013:2222::/64                                 1/20
     via 2003:1111::1, vlan3
E2 2014:2222::/64                                 1/20
     via 2003:1111::1, vlan3
E2 2015:2222::/64                                 1/20
     via 2003:1111::1, vlan3
```

show ipv6 ospf virtual-links

Overview Use this command in User Exec or Privileged Exec modes to display virtual link information, including OSPFv3 Authentication status for virtual links.

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

Syntax

```
show ipv6 ospf virtual-links
```

Mode User Exec and Privileged Exec

Usage notes See the OSPFv3 Feature Overview and Configuration Guide for more information and examples.

Examples To display virtual link information, use the command:

```
awplus# show ipv6 ospf virtual-links
```

Output Figure 29-17: Example output from the **show ipv6 ospf virtual-links** command showing OSPFv3 Authentication configuration information highlighted in bold

```
awplus#show ipv6 ospf virtual-links
 Virtual Link VLINK1 to router 192.168.1.10 is down
   Transit area 0.0.0.1 via interface *, instance ID 0
   Local address
   Remote address
   MD5 Authentication SPI 1000
   NULL encryption SHA-1 auth SPI 1001
   Transmit Delay is 1 sec, State Down,
   Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
     Hello due in inactive
     Adjacency state Down
```

Related commands

area virtual-link authentication ipsec spi

area virtual-link encryption ipsec spi

summary-address (IPv6 OSPF)

Overview Use this command in Router Configuration mode to summarize, or possibly suppress, external redistributed OSPFv3 routes within the specified address range.

Use the **no** variant of this command in Router Configuration mode to stop summarizing, or suppressing, external redistributed OSPFv3 routes within the specified address range.

Syntax

```
summary-address <ipv6-addr/prefix-length> [not-advertise] [tag
<0-4294967295>]
```

```
no summary-address <ipv6-addr/prefix-length> [not-advertise]
[tag <0-4294967295>]
```

Parameter	Description
<ipv6-addr/prefix-length>	Specifies the base IPv6 address of the IPv6 summary address. The range of addresses given as IPv6 starting address and an IPv6 prefix length.
`not-advertise`	Set the **not-advertise** option if you do not want OSPFv3 to advertise either the summary address or the individual networks within the range of the summary address.
`tag <0-4294967295>`	The tag parameter specifies the tag value that OSPFv3 places in the AS external LSAs created as a result of redistributing the summary route. The tag overrides tags set by the original route.

Default The default tag value for a summary address is 0.

Mode Router Configuration

Usage An address range is a pairing of an address and a prefix length. Redistributing routes from other protocols into OSPFv3 requires the router to advertise each route individually in an external LSA. Use this command to advertise one summary route for all redistributed routes covered by a specified prefix to decrease the size of the OSPFv3 link state database.

For example, if the specified address range is 2001:0db8:44::/48, then summary-address functionality will match 2001:0db8:4400:0000::1/128 through 2001:0db8:44ff:ffff::1/128.

Ensure OSPFv3 routes exist in the summary address range for advertisement before using this command.

Example The following example uses the `summary-address` command to aggregate external LSAs that match the IPv6 prefix `2001:0db8::/32` and assigns a tag value of `3`.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# summary-address 2001:0db8::/32 tag 3
```

The following example uses the `no summary-address` command to stop summarizing IPv6 addresses in the address range covered within the IPv6 prefix `2001:0db8::/32`.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no summary-address 2001:0db8::/32
```

timers spf exp (IPv6 OSPF)

Overview Use this command to adjust route calculation timers using exponential back-off delays.

Use **no** form of this command to return to the default exponential back-off timer values.

Syntax

```
timers spf exp <min-holdtime> <max-holdtime>
no timers spf exp <min-holdtime> <max-holdtime>
```

Parameter	Description
<min-holdtime>	Specifies the minimum delay between receiving a change to the SPF calculation in milliseconds. The range is 0-2147483647. The default SPF min-holdtime value is 50 milliseconds.
<max-holdtime>	Specifies the maximum delay between receiving a change to the SPF calculation in milliseconds. The range is 0-2147483647. The default SPF max-holdtime value is 50 seconds.

Mode Router Configuration

Usage notes This command configures the minimum and maximum delay time between the receipt of a topology change and the calculation of the Shortest Path First (SPF).

The time between SPF runs increases if a topology change occurs (and triggers a new SPF run) before the last SPF holdtimer has finished. The time between runs may increase up to the max-holdtime value.This increase in holdtime prevents too many SPF runs from occurring if multiple OSPF topology change events occur.

Examples To set the minimum delay time to 5 milliseconds and maximum delay time to 2 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# timers spf exp 5 2000
```

Related commands show ipv6 ospf

undebug ipv6 ospf events

Overview This command applies the functionality of the no debug ipv6 ospf events command.

undebug ipv6 ospf ifsm

Overview This command applies the functionality of the no debug ipv6 ospf ifsm command.

undebug ipv6 ospf lsa

Overview This command applies the functionality of the no debug ipv6 ospf lsa command.

undebug ipv6 ospf nfsm

Overview This command applies the functionality of the no debug ipv6 ospf nfsm command.

undebug ipv6 ospf packet

Overview This command applies the functionality of the no debug ipv6 ospf packet command.

undebug ipv6 ospf route

Overview This command applies the functionality of the no debug ipv6 ospf route command.

30 BGP and BGP4+ Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure the Border Gateway Protocol for IPv4 (BGP) and for IPv6 (BGP4+).

For basic BGP and BGP4+ introduction information and configuration examples, see the Routing_Protocol Guide.

Command List

- "address-family" on page 1279
- "aggregate-address" on page 1281
- "auto-summary (BGP only)" on page 1284
- "bgp aggregate-nexthop-check" on page 1286
- "bgp always-compare-med" on page 1287
- "bgp bestpath as-path ignore" on page 1289
- "bgp bestpath compare-confed-aspath" on page 1290
- "bgp bestpath compare-routerid" on page 1291
- "bgp bestpath med" on page 1292
- "bgp bestpath med remove-recv-med" on page 1294
- "bgp bestpath med remove-send-med" on page 1295
- "bgp client-to-client reflection" on page 1296
- "bgp cluster-id" on page 1297
- "bgp confederation identifier" on page 1299
- "bgp confederation peers" on page 1300
- "bgp config-type" on page 1302
- "bgp dampening" on page 1304
- "bgp damp-peer-oscillation (BGP only)" on page 1306

- "bgp default ipv4-unicast" on page 1307
- "bgp default local-preference (BGP only)" on page 1308
- "bgp deterministic-med" on page 1309
- "bgp enforce-first-as" on page 1311
- "bgp fast-external-failover" on page 1312
- "bgp graceful-restart" on page 1313
- "bgp graceful-restart graceful-reset" on page 1315
- "bgp log-neighbor-changes" on page 1316
- "bgp memory maxallocation" on page 1318
- "bgp nexthop-trigger-count" on page 1319
- "bgp nexthop-trigger delay" on page 1320
- "bgp nexthop-trigger enable" on page 1321
- "bgp rfc1771-path-select (BGP only)" on page 1322
- "bgp rfc1771-strict (BGP only)" on page 1323
- "bgp router-id" on page 1324
- "bgp scan-time (BGP only)" on page 1326
- "bgp update-delay" on page 1327
- "clear bgp *" on page 1328
- "clear bgp (IPv4 or IPv6 address)" on page 1329
- "clear bgp (ASN)" on page 1331
- "clear bgp external" on page 1332
- "clear bgp peer-group" on page 1333
- "clear bgp ipv6 (ipv6 address) (BGP4+ only)" on page 1334
- "clear bgp ipv6 dampening (BGP4+ only)" on page 1335
- "clear bgp ipv6 flap-statistics (BGP4+ only)" on page 1336
- "clear bgp ipv6 (ASN) (BGP4+ only)" on page 1337
- "clear bgp ipv6 external (BGP4+ only)" on page 1338
- "clear bgp ipv6 peer-group (BGP4+ only)" on page 1339
- "clear ip bgp * (BGP only)" on page 1340
- "clear ip bgp (IPv4) (BGP only)" on page 1341
- "clear ip bgp dampening (BGP only)" on page 1342
- "clear ip bgp flap-statistics (BGP only)" on page 1343
- "clear ip bgp (ASN) (BGP only)" on page 1344
- "clear ip bgp external (BGP only)" on page 1345
- "clear ip bgp peer-group (BGP only)" on page 1346

- "clear ip prefix-list" on page 1347
- "debug bgp (BGP only)" on page 1348
- "distance (BGP and BGP4+)" on page 1350
- "exit-address-family" on page 1352
- "ip as-path access-list" on page 1353
- "ip community-list" on page 1355
- "ip community-list expanded" on page 1357
- "ip community-list standard" on page 1359
- "ip extcommunity-list expanded" on page 1361
- "ip extcommunity-list standard" on page 1363
- "ip prefix-list" on page 1365
- "ipv6 prefix-list" on page 1367
- "match as-path" on page 1369
- "match community" on page 1371
- "max-paths" on page 1373
- "neighbor activate" on page 1374
- "neighbor advertisement-interval" on page 1377
- "neighbor allowas-in" on page 1380
- "neighbor as-origination-interval" on page 1383
- "neighbor attribute-unchanged" on page 1385
- "neighbor capability graceful-restart" on page 1388
- "neighbor capability orf prefix-list" on page 1391
- "neighbor capability route-refresh" on page 1394
- "neighbor collide-established" on page 1397
- "neighbor default-originate" on page 1400
- "neighbor description" on page 1403
- "neighbor disallow-infinite-holdtime" on page 1406
- "neighbor distribute-list" on page 1408
- "neighbor dont-capability-negotiate" on page 1411
- "neighbor ebgp-multihop" on page 1414
- "neighbor enforce-multihop" on page 1417
- "neighbor filter-list" on page 1420
- "neighbor interface" on page 1423
- "neighbor local-as" on page 1424
- "neighbor maximum-prefix" on page 1427

- "neighbor next-hop-self" on page 1430
- "neighbor override-capability" on page 1433
- "neighbor passive" on page 1435
- "neighbor password" on page 1438
- "neighbor peer-group (add a neighbor)" on page 1441
- "neighbor peer-group (create a peer-group)" on page 1443
- "neighbor port" on page 1444
- "neighbor prefix-list" on page 1447
- "neighbor remote-as" on page 1450
- "neighbor remove-private-AS (BGP only)" on page 1453
- "neighbor restart-time" on page 1455
- "neighbor route-map" on page 1458
- "neighbor route-reflector-client (BGP only)" on page 1462
- "neighbor route-server-client (BGP only)" on page 1464
- "neighbor send-community" on page 1465
- "neighbor shutdown" on page 1469
- "neighbor soft-reconfiguration inbound" on page 1471
- "neighbor timers" on page 1474
- "neighbor transparent-as" on page 1477
- "neighbor transparent-nexthop" on page 1479
- "neighbor unsuppress-map" on page 1481
- "neighbor update-source" on page 1484
- "neighbor version (BGP only)" on page 1488
- "neighbor weight" on page 1490
- "network (BGP and BGP4+)" on page 1493
- "network synchronization" on page 1496
- "redistribute (into BGP or BGP4+)" on page 1497
- "restart bgp graceful (BGP only)" on page 1499
- "router bgp" on page 1500
- "route-map" on page 1501
- "set as-path" on page 1504
- "set community" on page 1505
- "show bgp ipv6 (BGP4+ only)" on page 1507
- "show bgp ipv6 community (BGP4+ only)" on page 1508
- "show bgp ipv6 community-list (BGP4+ only)" on page 1510

- "show bgp ipv6 dampening (BGP4+ only)" on page 1511
- "show bgp ipv6 filter-list (BGP4+ only)" on page 1512
- "show bgp ipv6 inconsistent-as (BGP4+ only)" on page 1513
- "show bgp ipv6 longer-prefixes (BGP4+ only)" on page 1514
- "show bgp ipv6 neighbors (BGP4+ only)" on page 1515
- "show bgp ipv6 paths (BGP4+ only)" on page 1518
- "show bgp ipv6 prefix-list (BGP4+ only)" on page 1519
- "show bgp ipv6 quote-regexp (BGP4+ only)" on page 1520
- "show bgp ipv6 regexp (BGP4+ only)" on page 1521
- "show bgp ipv6 route-map (BGP4+ only)" on page 1523
- "show bgp ipv6 summary (BGP4+ only)" on page 1524
- "show bgp memory maxallocation (BGP only)" on page 1525
- "show bgp nexthop-tracking (BGP only)" on page 1526
- "show bgp nexthop-tree-details (BGP only)" on page 1527
- "show debugging bgp (BGP only)" on page 1528
- "show ip bgp (BGP only)" on page 1529
- "show ip bgp attribute-info (BGP only)" on page 1530
- "show ip bgp cidr-only (BGP only)" on page 1531
- "show ip bgp community (BGP only)" on page 1532
- "show ip bgp community-info (BGP only)" on page 1534
- "show ip bgp community-list (BGP only)" on page 1535
- "show ip bgp dampening (BGP only)" on page 1536
- "show ip bgp filter-list (BGP only)" on page 1538
- "show ip bgp inconsistent-as (BGP only)" on page 1539
- "show ip bgp longer-prefixes (BGP only)" on page 1540
- "show ip bgp neighbors (BGP only)" on page 1541
- "show ip bgp neighbors connection-retrytime (BGP only)" on page 1544
- "show ip bgp neighbors hold-time (BGP only)" on page 1545
- "show ip bgp neighbors keepalive (BGP only)" on page 1546
- "show ip bgp neighbors keepalive-interval (BGP only)" on page 1547
- "show ip bgp neighbors notification (BGP only)" on page 1548
- "show ip bgp neighbors open (BGP only)" on page 1549
- "show ip bgp neighbors rcvd-msgs (BGP only)" on page 1550
- "show ip bgp neighbors sent-msgs (BGP only)" on page 1551
- "show ip bgp neighbors update (BGP only)" on page 1552

- "show ip bgp paths (BGP only)" on page 1553
- "show ip bgp prefix-list (BGP only)" on page 1554
- "show ip bgp quote-regexp (BGP only)" on page 1555
- "show ip bgp regexp (BGP only)" on page 1557
- "show ip bgp route-map (BGP only)" on page 1559
- "show ip bgp scan (BGP only)" on page 1560
- "show ip bgp summary (BGP only)" on page 1561
- "show ip community-list" on page 1562
- "show ip extcommunity-list" on page 1563
- "show ip prefix-list" on page 1564
- "show ipv6 prefix-list" on page 1565
- "show ip protocols bgp (BGP only)" on page 1566
- "show route-map" on page 1567
- "synchronization" on page 1568
- "timers (BGP)" on page 1570
- "undebug bgp (BGP only)" on page 1572

address-family

Overview This command enters the IPv4 or IPv6 Address-Family Configuration command mode. In this mode you can configure address-family specific parameters.

Syntax [BGP]

```
address-family ipv4 [unicast]
no address-family ipv4 [unicast]
```

Syntax [BGP4+]

```
address-family ipv6 [unicast]
no address-family ipv6 [unicast]
```

Parameter	Description
ipv4	Configure parameters relating to the exchange of IPv4 prefixes.
ipv6	Configure parameters relating to the exchange of IPv6 prefixes.
unicast	Configure parameters relating to the exchange of routes to unicast destinations.

Mode [BGP] Router Configuration

Mode [BGP4+] Router Configuration

Usage notes To leave the IPv4 or IPv6 Address Family Configuration mode, and return to the Router Configuration mode, use the exit-address-family command.

Example [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# neighbor 192.168.0.1 remote-as 100
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 192.168.0.1 activate
awplus(config-router-af)# exit-address-family
awplus(config-router)#
```

Example [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1 activate
awplus(config-router-af)# exit-address-family
awplus(config-router)#
```

Related commands exit-address-family

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

aggregate-address

Overview This command adds an aggregate route that can be advertised to BGP or BGP4+ neighbors. This command creates an aggregate entry in the BGP or BGP4+ routing table if the device learns, by any means, any routes that are within the range configured by the aggregate address/mask.

When this command is used with the **summary-only** option, the more-specific routes of the aggregate are suppressed to all neighbors. Use the neighbor unsuppress-map command instead to selectively leak more-specific routes to a particular neighbor.

The **no** variant of this command removes the aggregate configured by the **aggregate-address** command.

Syntax [BGP]

```
aggregate-address <ip-addr/m> {summary-only|as-set}
no aggregate-address <ip-addr/m> {summary-only|as-set}
```

Syntax [BGP4+]

```
aggregate-address <ipv6-addr/prefix-length>
{summary-only|as-set}
no aggregate-address <ipv6-addr/prefix-length>
{summary-only|as-set}
```

Parameter	Description
<ip-addr/m>	Specifies the aggregate IPv4 address and mask.
<ipv6-addr/prefix-length>	Specifies the aggregate IPv6 address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
`summary-only`	Filters more specific routes from updates. Only the aggregate address/mask will be advertised, and none of the component addresses that fall within the range of the aggregate address/mask.
`as-set`	Generates AS set path information. The AS-path advertised with the aggregate is an unordered list of all the AS-numbers that appear in any of the AS-paths of the component routes, with each AS-number appearing just once in the list.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage [BGP] If the `summary-only` parameter is specified, then only the aggregate address/mask will be advertised, and none of the component addresses that fall within the range of the aggregate address/mask. For example, if you configure:

```
awplus# configure terminal

awplus(config)# router bgp 100

awplus(config-router)# aggregate-address 172.0.0.0/8 summary-
only
```

then the device will advertise the prefix `172.0.0.0/8`, but no component routes like `172.10.0.0/16`

The `as-set` parameter controls the AS-path attribute that is advertised with the aggregate route. If the device has learned multiple routes that are within the range of the aggregate address/mask, and the AS-paths associated with those routes contain different sets of AS-numbers, then it is not possible to create a single AS-path that accurately represents the AS-paths of all those component routes. In this case, the device will, by default, advertise a NULL AS-path with the aggregate.

Usage [BGP4+]

If the `summary-only` parameter is specified, then only the aggregate address/mask will be advertised, and none of the component addresses that fall within the range of the aggregate address/mask. For example, if you configure:

```
awplus# configure terminal

awplus(config)# router bgp 100

awplus(config-router)#address-family ipv6

awplus(config-router-af)# aggregate-address 2001:0db8::/64
summary-only
```

then the device will advertise the prefix 2001:0db8::/64, but no component routes like 2001:0db8:010d::1/128

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# aggregate-address 192.0.0.0/8 as-set
summary-only
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no aggregate-address 192.0.0.0/8 as-set
summary-only
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address family ipv6
awplus(config-router-af)# aggregate-address 2001:0db8::/64
as-set summary-only
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address family ipv6
awplus(config-router-af)# no aggregate-address 2001:0db8::/64
as-set summary-only
```

Related commands

aggregate-address

match as-path

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

auto-summary (BGP only)

Overview Use this command to enable sending summarized routes by a BGP speaker to its peers in the Router Configuration mode or in the Address-Family Configuration mode. BGP uses auto-summary to advertise summarized routes.

Use the **no** variant of this command to disable BGP auto-summary.

Syntax

```
auto-summary
no auto-summary
```

Default The auto-summary function is disabled by default.

Mode Router Configuration and Address Family IPv4 mode

Usage If certain routes have already been advertised, enabling auto-summary results in non- summarized routes being withdrawn and only summarized routes are advertised. Summarized routes are advertised before non-summarized routes are withdrawn from all connected peers.

If certain routes have already been advertised, disabling auto-summary results in summarized routes being withdrawn and only non-summarized routes are advertised. Non-summarized routes are advertised before summarized routes are withdrawn from all connected peers.

Examples The following example enables auto-summary in Router Configuration mode:

```
awplus# configure
awplus(config)# router bgp 100
awplus(config-router)# auto-summary
```

The following example disables auto-summary in Router Configuration mode:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no auto-summary
```

The following example enables auto-summary in Address Family IPv4 mode:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv4
awplus(config-router-af)# auto-summary
```

The following example disables auto-summary in Address Family IPv4 mode:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no auto-summary
```

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp aggregate-nexthop-check

Overview This command affects the operation of the summary-only option on the aggregate-address command.

This command enables a mode whereby the summary-only option will only suppress the component routes if those component routes all have the same next hop. If the routes have different next hops, then they will continue to be advertised to peers even if the summary-only option is configured. By default this is disabled.

The **no** variant of this command disables this function.

Syntax

```
bgp aggregate-nexthop-check
no bgp aggregate-nexthop-check
```

Default Disabled by default.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# bgp aggregate-nexthop-check
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp always-compare-med

Overview This command enables BGP to compare the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.

Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal.

By default, MED comparison is done only among routes from the same autonomous system (AS). Use the **bgp always-compare-mode** command to allow comparison of MEDs from different ASs.

A path with a lower MED value is preferred. For example, if the bgp table contains the following entries, and the **bgp always-compare-med** command has been issued to enable this feature:

- Route1: as-path 400, med 300
- Route2: as-path 200, med 200
- Route3: as-path 400, med 250

Route1 is compared to Route2. Route2 is best of the two (lower MED). Next, Route2 is compared to Route3 and Route2 is chosen best path again (lower MED). If **always-compare-med** was disabled, MED is not taken into account when Route1 and Route2 are compared, because of different ASs and MED is compared for only Route1 and Route3. In this case, Route3 would be the best path. The selected route is also affected by the **bgp deterministic-med** command. See the bgp deterministic-med command for details.

If this command is used to compare MEDs for all paths, it should be configured on every BGP router in the AS.

The **no** variant of this command disallows the comparison.

Syntax

```
bgp always-compare-med
no bgp always-compare-med
```

Default By default this feature is disabled.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp always-compare-med
```

Related commands

bgp bestpath med

bgp bestpath as-path ignore

bgp bestpath compare-routerid

bgp deterministic-med

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath as-path ignore

Overview This command prevents the router from considering as-path as a factor in the algorithm for choosing a route.

The **no** variant of this command allows the router to consider as-path in choosing a route.

Syntax
```
bgp bestpath as-path ignore
no bgp bestpath as-path ignore
```

Mode Router Configuration

Example
```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath as-path ignore
```

Related commands
bgp always-compare-med

bgp bestpath med

bgp bestpath compare-routerid

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath compare-confed-aspath

Overview This command specifies that the AS confederation path length must be used, when available, in the BGP best path decision process. It is effective only when bgp bestpath as-path ignore command has not been specified.

By default, if BGP receives routes with identical eBGP paths from eBGP peers, BGP does not continue to consider any AS confederation path length attributes that may be associated with the routes.

The **no** variant of this command returns the device to the default state, where the device ignores AS confederation path length in the BGP best path selection process.

Syntax
```
bgp bestpath compare-confed-aspath
no bgp bestpath compare-confed-aspath
```

Mode Router Configuration

Example
```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath compare-confed-aspath
```

Related commands bgp bestpath as-path ignore

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath compare-routerid

Overview

By default, when comparing similar routes from peers, BGP does not consider the router ID of neighbors advertising the routes - BGP simply selects the first received route. Use this command to include router ID in the selection process; similar routes are compared and the route with the lowest router ID is selected.

The **no** variant of this command disables this feature, and returns the device to the default state, where the device ignores the router ID in the BGP best path selection process.

Syntax

```
bgp bestpath compare-routerid
no bgp bestpath compare-routerid
```

Mode

Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath compare-routerid
```

Related commands

show ip bgp (BGP only)

show bgp ipv6 neighbors (BGP4+ only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath med

Overview This command controls how the Multi Exit Discriminator (MED) attribute comparison is performed.

Use the **no** variant of this command to prevent BGP from considering the MED attribute when comparing paths.

Syntax

```
bgp bestpath med {[confed] [missing-as-worst]}
```

Parameter	Description
`confed`	Compares MED among confederation paths.
`missing-as-worst`	Treats missing MED as the least preferred one.

Mode Router Configuration

Usage The **confed** parameter enables MED comparison among paths learned from confederation peers. The MED attributes are compared only if there is no external AS (Autonomous System), where an external AS is one that is not within the confederation. If there is an external AS in the path, then the MED comparison is not made.

For example, in the following paths the MED value is not compared with `Path3` since it is not in the confederation. MED is compared for `Path1` and `Path2` only.

- Path1 = 32000 32004, med=4
- Path2 = 32001 32004, med=2
- Path3 = 32003 1, med=1

The effect of the **missing-as-worst** parameter is to treat a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path. If the **missing-as-worst** parameter is not configured, the missing MED attribute is assigned the value of 0, making the path with the missing MED attribute the best path.

Examples

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath med missing-as-worst
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath med confed
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath med confed missing-as-worst
```

Related commands

bgp always-compare-med

bgp bestpath as-path ignore

bgp deterministic-med

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath med remove-recv-med

Overview This command removes the Multi Exit Discriminator (MED) attribute from the update messages received by the BGP speaker from its peers. However, the local BGP speaker will send MED attributes in the update messages to its peers, unless specified not to by the **bgp bestpath med remove-send-med** command.

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

Syntax

```
bgp bestpath med remove-recv-med
no bgp bestpath med remove-recv-med
```

Mode Router Configuration

Example To enable the **remove-recv-med** feature on the BGP speaker belonging to the Autonomous System (AS) 100, enter the command:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath med remove-recv-med
```

Related commands bgp bestpath med remove-send-med

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath med remove-send-med

Overview This command removes the Multi Exit Discriminator (MED) attribute from the update messages sent by the BGP speaker to its peers. However, the local BGP speaker will consider the MED attribute received from other peers during the decision and route selection process, unless specified not to by the **bgp bestpath med remove-recv-med** command.

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

Syntax

```
bgp bestpath med remove-send-med
no bgp bestpath med remove-send-med
```

Mode Router Configuration

Example To enable the **remove-send-med** feature on the BGP speaker belonging to the Autonomous System (AS) 100, enter the command:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath med remove-send-med
```

Related commands bgp bestpath med remove-recv-med

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp client-to-client reflection

Overview This command restores route reflection from a BGP route reflector to clients, and is used to configure routers as route reflectors. Route reflectors are used when all Interior Border Gateway Protocol (iBGP) speakers are not fully meshed.

If the clients are fully meshed the route reflector is not required, use the **no** variant of this command to disable the client-to-client route reflection.

When a router is configured as a route reflector, client-to-client reflection is enabled by default.

The **no** variant of this command turns off client-to-client reflection.

Syntax
```
bgp client-to-client reflection
no bgp client-to-client reflection
```

Default This command is enabled by default.

Mode Router Configuration

Example
```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp client-to-client reflection
```

Related commands
bgp cluster-id

neighbor route-reflector-client (BGP only)

show bgp ipv6 (BGP4+ only)

show ip bgp (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp cluster-id

Overview This command configures the cluster-id if the BGP cluster has more than one route reflector. A cluster includes one or more route reflectors and their clients. Usually, each cluster is identified by the router-id of its single route reflector. However, to increase redundancy, a cluster may sometimes have more than one route reflector. All router reflectors in such a cluster are then identified by a cluster-id.

The **bgp cluster-id** command is used to configure the 4 byte cluster ID for clusters with more than one route reflector.

The **no** variant of this command removes the cluster ID.

Syntax

```
bgp cluster-id {<ip-address>|<cluster-id>}
no bgp cluster-id
```

Parameter	Description	
<cluster-id>	<1-4294967295>	Route Reflector cluster-id as a 32 bit quantity.
<ip-address>	*A.B.C.D*	Route Reflector Cluster-id in IP address format.

Mode Router Configuration

Usage The following configuration creates `cluster-id 5` including two route-reflector- clients.

```
awplus(config)# router bgp 200
awplus(config-router)# neighbor 2.2.2.2 remote-as 200
awplus(config-router)# neighbor 3.3.3.3 remote-as 200
awplus(config-router)# neighbor 3.3.3.3 route-reflector-client
awplus(config-router)# neighbor 5.5.5.5 remote-as 200
awplus(config-router)# neighbor 5.5.5.5 route-reflector-client
awplus(config-router)# neighbor 6.6.6.6 remote-as 200
awplus(config-router)# bgp cluster-id 5
```

Examples To add a **bgp cluster-id**, apply the example commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp cluster-id 10.10.1.1
```

To remove a bgp cluster-id apply the example commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp cluster-id 10.10.1.1
```

Related commands

bgp client-to-client reflection

neighbor route-reflector-client (BGP only)

show bgp ipv6 (BGP4+ only)

show ip bgp (BGP only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp confederation identifier

Overview This command specifies a BGP confederation identifier.

The **no** variant of this command removes all BGP confederation identifiers.

Syntax

```
bgp confederation identifier <1-4294967295>
no bgp confederation identifier
```

Parameter	Description
<1-4294967295>	Set routing domain confederation AS number.

Mode Router Configuration

Examples

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp confederation identifier 1
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp confederation identifier
```

Related commands bgp confederation peers

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp confederation peers

Overview This command configures the Autonomous Systems (AS) that belong to the same confederation as the current device.

A confederation allows an AS to be divided into several sub-ASs. The overall AS is given a confederation identifier. External routers view only the whole confederation as one AS, whose AS number is the confederation identifier. Each sub-AS is fully meshed within itself and is visible internally to the confederation.

Use the **bgp confederation peer** command to define the list of AS numbers of the sub-ASs in the confederation containing the current device.

The **no** variant of this command removes an autonomous system from the confederation.

Syntax

```
bgp confederation peers <1-4294967295>
no bgp confederation peers <1-4294967295>
```

Parameter	Description
<1-4294967295>	AS numbers of eBGP peers that are under same confederation but in a different sub-AS.

Mode Router Configuration

Usage notes In the following configuration of **Router 1** the neighbor `172.210.30.2` and `172.210.20.1` have iBGP connection within AS `100`. The neighbor `173.213.30.1` has an BGP connection, but it is within AS `200`, which is part of the same confederation. The neighbor `6.6.6.6` has an eBGP connection to external AS `500`.

In the configuration of **Router 2**, neighbor `5.5.5.4` has an eBGP connection to confederation `300`. `Router2` does not know about the ASs `100` and `200`, it only knows about confederation `300`.

Router 1

```
awplus(config)# router bgp 100
awplus(config-router)# bgp confederation identifier 300
awplus(config-router)# bgp confederation peers 200
awplus(config-router)# neighbor 172.210.30.2 remote-as 100
awplus(config-router)# neighbor 172.210.20.1 remote-as 100
awplus(config-router)# neighbor 173.213.30.1 remote-as 200
awplus(config-router)# neighbor 6.6.6.6 remote-as 300
```

Router 2

```
awplus(config)# router bgp 500
awplus(config-router)# neighbor 5.5.5.4 remote-as 300
```

Example

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp confederation peers 1234
```

Related commands

bgp confederation identifier

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp config-type

Overview Use this command to set the BGP configuration type to either **standard** or **enhanced** types. When you configure the **enhanced** type, then BGP and BGP4+ communities are allowed to be sent and received by default. The **enhanced** type is configured by default.

Use the **no** variant of this command to restore the default BGP configuration type (**enhanced**).

Syntax

```
bgp config-type {standard|enhanced}
no bgp config-type
```

Parameter	Description
`standard`	Specifies the industry standard style configuration. After setting the configuration to standard, make sure to use the neighbor send-community command to send out BGP community attributes. The synchronization command is enabled in the Global Configuration mode and is shown in the configuration.
`enhanced`	Specifies the enhanced style configuration. The enhanced configuration type requires no specific configuration for sending out BGP standard community and extended community attributes. The synchronization command is enabled by default in the Global Configuration mode and is not shown in configuration output.

Default By default, the BGP configuration type is **enhanced**.

Mode Global Configuration

Usage notes Note that the **enhanced** type default configuration may cause issues in some networks if unauthorized BGP peers are advertising BGP communities to adjust routing decisions.

Changing modes requires you to **reload** your device for the change to take effect:

```
awplus(config)#bgp config-type standard
awplus(config)#exit
awplus#reload
reboot system? (y/n): y
```

When your device reloads, it will load with the standard BGP settings commonly used by most vendors. Apply the **standard** type configuration if you have interoperability issues.

Examples To specify the `standard` BGP configuration type, enter the following commands:

```
awplus# configure terminal
awplus(config)# bgp config-type standard
```

To specify the `enhanced` BGP configuration type, enter the following commands:

```
awplus# configure terminal
awplus(config)# bgp config-type enhanced
```

To restore the default BGP configuration type (`enhanced`), enter the following commands:

```
awplus# configure terminal
awplus(config)# no bgp config-type
```

Related commands

neighbor send-community

synchronization

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp dampening

Overview This command enables BGP and BGP4+ dampening and sets BGP and BGP4+ dampening parameters. BGP4+ dampening is available from the IPv6 Address Family Configuration mode. BGP dampening is available from the Router Configuration mode.

The **no** variant of this command disables BGP dampening or unsets the BGP dampening parameters.

Syntax

```
bgp dampening
no bgp dampening
bgp dampening <reachtime>
no bgp dampening <reachtime>
bgp dampening <reachtime> <reuse> <suppress> <maxsuppress> <unreachtime>
no bgp dampening <reachtime> <reuse> <suppress> <maxsuppress> <unreachtime>
bgp dampening route-map <routemap-name>
no bgp dampening route-map <routemap-name>
```

Parameter	Description
<reachtime>	<1-45> Specifies the reachability half-life time in minutes. The time for the penalty to decrease to one-half of its current value. The default is 15 minutes.
<reuse>	<1-20000> Specifies the reuse limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed. The default reuse limit is 750
<suppress>	<1-20000> Specifies the suppress limit value. When the penalty for a route exceeds the suppress value, the route is suppressed. The default suppress limit is 2000.
<maxsuppress>	<1-255> Specifies the max-suppress-time. Maximum time that a dampened route is suppressed. The default max-suppress value is 4 times the half-life time (60 minutes).
<unreachtime>	<1-45> Specifies the un-reachability half-life time for penalty, in minutes.
route-map	Route-map to specify criteria for dampening.
<routemap-name>	Specify the name of the route-map.

Mode [BGP] Router Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage notes Route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the **suppress** limit the advertisement of the route is suppressed. This penalty is decayed according to the configured **half time** value. Once the penalty is lower than the **reuse** limit, the route advertisement is un-suppressed.

The dampening information is purged from the router once the penalty becomes less than half of the **reuse** limit.

Example [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# bgp dampening 20 800 2500 80 25
```

Example [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# address-family ipv6
awplus(config-router-af)# bgp dampening 20 800 2500 80 25
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp damp-peer-oscillation (BGP only)

Overview Use this command to enable BGP peer oscillating connection damping.

Use the **no** variant of this command to disable BGP peer oscillating connection damping.

Syntax

```
bgp damp-peer-oscillations
no bgp damp-peer-oscillations
```

Default By default, this functionality is enabled and will not appear in the **show running-config** command output.

Mode Router Configuration

Usage BGP peers in AlliedWare Plus will automatically attempt to form connections with configured neighbors. Due to misconfiguration these connections may fail and continue to fail until such time as the misconfiguration is detected and fixed. During this time, BGP can quickly cycle through the state machine from Idle through the various Connect states, which can result in large numbers of TCP sessions being opened in a short period of time.

This command instead adds a delay after a peer enters the Idle state before it can progress to the later states. The default delay is 0 second, increasing by 1 second for each unsuccessful connection attempt, to a maximum of 5 seconds. After a successful BGP route update has been received over a connection, the delay will be reset to 0. This command implements the DampPeerOscillations FSM behavior described in section 8.1 of RFC 4271.

The command is enabled by default. When disabled, peers will transition out of the Idle state immediately. The command applies globally to all currently configured BGP peers and all future peers to be created.

Example To disable peer connection damping, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 1
awplus(config-router)# no bgp damp-peer-oscillations
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp default ipv4-unicast

Overview This command configures BGP defaults and activates IPv4-unicast for a peer by default. This affects BGP global configuration. By default, BGP exchanges IPv4 prefixes with a peer.

The **no** variant of this command disables this function. The BGP routing process will no longer exchange IPv4 addressing information with BGP neighbor routers. Note that disabling the exchange of IPv4 prefixes will also enable an IPv6 only BGP4+ network.

Syntax
```
bgp default ipv4-unicast
no bgp default ipv4-unicast
```

Default This is enabled by default.

Mode Router Configuration

Usage Use the negated form of this command to enable an IPv6 only BGP4+ network.

Examples
```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp default ipv4-unicast
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp default ipv4-unicast
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp default local-preference (BGP only)

Overview This command changes the default local preference value.

The local preference indicates the preferred path when there are multiple paths to the same destination. The path with the higher preference is preferred.

Use this command to define the default local preference value that the device will advertise for the routes it sends. The preference is sent to all routers and access servers in the local autonomous system.

The **no** variant of this command reverts to the default local preference value of 100.

Syntax

```
bgp default local-preference <pref-value>
no bgp default local-preference [<pref-value>]
```

Parameter	Description
<pref-value>	<0-4294967295> Configure default local preference value. The default local preference value is 100.

Default By default the local-preference value is 100.

Mode Router Configuration

Examples

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp default local-preference 2345555
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp default local-preference
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp deterministic-med

Overview Use this command to allow or disallow the device to compare the Multi Exit Discriminator (MED) variable when choosing among routes advertised by different peers in the same autonomous system (AS).

Use the **bgp deterministic-med** command to enable this feature to allow the comparison of MED variables when choosing among routes advertised by different peers in the same AS.

Use the **no** variant of this command to disable this feature to disallow the comparison of the MED variable when choosing among routes advertised by different peers in the same AS.

Syntax

```
bgp deterministic-med
no bgp deterministic-med
```

Default Disabled

Mode Router Configuration

Usage When the **bgp deterministic-med** command is enabled, routes from the same AS are grouped together and ordered according to their MED values, and the best routes of each group are compared.

The main benefit of this is that the choice of best route then does not depend on the order in which the routes happened to be received, which is rather random and arbitrary.

To see how this works, consider the following set of bgp table entries, all for the same route:

```
1: ASPATH 234, MED 120, internal, IGP metric to NEXT_HOP 40
2: ASPATH 389, MED 190, internal, IGP metric to NEXT_HOP 35
3: ASPATH 234, MED 245, external
```

If **bgp deterministic-med** is not enabled, then entry `3` will be chosen, because it is an external route.

But if BGP deterministic-MED is enabled, the entries will be grouped as follows:

```
Group 1:  1: ASPATH 234, MED 120, internal, IGP metric to NEXT_HOP 40
          3: ASPATH 234, MED 245, external
Group 2:  2: ASPATH 389, MED 190, internal, IGP metric to NEXT_HOP 35
```

NOTE: *Routes from the same AS are grouped together and ordered by MED.*

Entry `1` is chosen as the best route from `Group 1`, since this route has the lowest MED value. Entry 2 has to be the best route in `Group 2`, since this is the only route in that group. These two group winners are compared against each other, and

Entry 2 is chosen as the best route because Entry 2 has the lower metric to next-hop.

All routers in an AS should have the same setting for BGP deterministic-MED. All routers in an AS should have BGP deterministic-MED enabled with **bgp deterministic-med**, or all routers in an AS should have BGP deterministic-MED disabled with **no bgp-deterministic- med**.

In the example above, the MED values were not considered when comparing the winners of the two groups (the best routes from the different ASs). To use MED in the comparison of routes from different ASs, use the bgp always-compare-med command.

Examples

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp deterministic-med
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp deterministic-med
```

Related commands

show ip bgp (BGP only)

show bgp ipv6 neighbors (BGP4+ only)

show ip bgp neighbors (BGP only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp enforce-first-as

Overview Use this command to enforce the denying of eBGP updates in which the neighbor's AS number is not the first AS in the AS-path attribute.

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

Syntax
```
bgp enforce-first-as
no bgp enforce-first-as
```

Mode Router Configuration

Usage This command specifies that any updates received from an external neighbor that do not have the neighbor's configured Autonomous System (AS) at the beginning of the AS_PATH in the received update must be denied. Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.

Example
```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router# bgp enforce-first-as
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp fast-external-failover

Overview Use this command to reset a BGP session immediately if the interface used for BGP connection goes down.

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

Syntax
```
bgp fast-external-failover
no bgp fast-external-failover
```

Default Enabled

Mode Router Configuration

Example
```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp fast-external-failover
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp graceful-restart

Overview Use this command to enable BGP and BGP4+ graceful-restart capabilities for restart and stalepath times.

Use the **no** variant of this command to restore restart timers to their default settings.

Syntax

```
bgp graceful-restart [restart-time <delay-value>|
stalepath-time <delay-value>]
```

```
no bgp graceful-restart [restart-time|stalepath-time]
```

Parameter	Description
`restart-time`	The maximum time needed for neighbors to restart, in seconds. The default restart-time is 120 seconds.
`stalepath-time`	The maximum time to retain stale paths from restarting neighbors, in seconds. The default stalepath-time is 120 seconds.
`<delay-value>`	<1-3600> Maximum time in seconds.

Default Graceful restart is disabled by default. If you enable it and do not specify the restart-time and stalepath-time, they default to 120 seconds.

Mode Router Configuration

Usage notes The **restart-time** parameter is used for setting the maximum time that a graceful-restart neighbor waits to come back up after a restart. This **restart-time** value is applied to neighbors unless you explicitly override it by configuring the corresponding value on the neighbor.

The **stalepath-time** parameter is used to set the maximum time to preserve stale paths from a gracefully restarted neighbor. All stalepaths, unless reinstated by the neighbor after a re-establishment, will be deleted when time, as specified by the **stalepath-time** parameter, expires.

Examples To enable graceful restart, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# bgp graceful-restart
```

To disable graceful restart, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no bgp graceful-restart
```

To enable graceful restart and set the restart time to 150 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# bgp graceful-restart restart-time 150
```

To return the restart-time to its default of 120 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no bgp graceful-restart restart-time
```

Related commands

bgp graceful-restart graceful-reset

restart bgp graceful (BGP only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp graceful-restart graceful-reset

Overview This command enables BGP and BGP4+ graceful-restart when a configuration change forces a peer restart.

Use the **no** variant of this command to restore the device to its default state.

Syntax

```
bgp graceful-restart graceful-reset
no bgp graceful-restart graceful-reset
```

Default Disabled

Mode Router Configuration

Usage The bgp graceful-restart command must be enabled before this command is enabled. All events that cause BGP peer reset, including all session reset commands, can trigger graceful-restart.

Example To enable the graceful-restart graceful-reset feature on the BGP or BGP4+ peer belonging to Autonomous System (AS) 10, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# bgp graceful-restart graceful-reset
```

To disable the graceful-restart graceful-reset feature on the BGP or BGP4+ peer belonging to Autonomous System (AS) 10, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no bgp graceful-restart graceful-reset
```

Related commands bgp graceful-restart

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp log-neighbor-changes

Overview Use this command to enable logging of status change messages without turning on **debug bgp** commands.

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

Syntax

```
bgp log-neighbor-changes
no bgp log-neighbor-changes
```

Default Disabled

Mode Router Configuration

Usage notes AlliedWare Plus™ provides other kinds of logging services for neighbor status, for example, **debug bgp fsm** and **debug bgp events**.

However, these commands create a significant hit in the logging performance. If you need to log neighbor status changes only, we recommend turning off all the debug commands, and then use this command.

To see BGP neighbor changes in the log you must also set the log level to informational using the **log buffered** command.

A sample output of this log is:

```
%Protocol-Severity-Events: Message-text
```

A sample output of the log for an interface down event is:

```
%BGP-5-ADJCHANGE: neighbor 10.10.0.24 Down Interface flap
```

The **bgp log-neighbor-changes** command logs the following events:

- BGP Notification Received
- Erroneous BGP Update Received
- User reset request
- Peer time-out
- Peer Closing down the session
- Interface flap
- Router ID changed
- Neighbor deleted
- Member added to peer group
- Administrative shutdown

- Remote AS changed
- RR client configuration modification
- Soft reconfiguration modification

Example To enable the logging of BGP status changes without using the debug bgp command:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp log-neighbor-changes
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp memory maxallocation

Overview This command allocates a maximum percentage of the RAM (Random Access Memory) available on the device for BGP processes.

When this percentage is exceeded, BGP peering terminates and an **out of resources** error displays. The default setting for **bgp memory maxallocation** is 100% memory allocation.

Use the **no** variant of this command to reset memory allocation to the default.

Syntax

```
bgp memory maxallocation <1-100>
no bgp memory maxallocation
```

Parameter	Description
<1-100>	Percentage of device memory allocated to BGP processes. Note this is RAM (Random Access Memory), not device flash memory.

Default BGP processes are allocated the maximum percentage of 100% of the device's available RAM memory by default. Note only non-default BGP memory allocation values are shown in the running or startup configuration files:

```
awplus#show running-config
!
bgp memory maxallocation 50
!
```

Mode Global Configuration

Examples To limit the maximum amount of memory used by BGP processes to 65% of the total RAM memory available on the device, use the commands:

```
awplus# configure terminal
awplus(config)# bgp memory maxallocation 65
```

To return to the default 100% maximum RAM memory allocation available on the device for BGP processes, use the commands:

```
awplus# configure terminal
awplus(config)# no bgp memory maxallocation
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp nexthop-trigger-count

Overview Use this command to configure the display of BGP next hop tracking status.

Use the **no** variant of this command to disable this function.

Syntax

```
bgp nexthop-trigger-count <0-127>
no bgp nexthop-trigger-count
```

Parameter	Description
<0-127>	BGP next hop tracking status.

Mode Router Configuration

Example To enable next-hop-tracking status on the BGP peer belonging to the Autonomous System (AS) 100, enter the following commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp nexthop-trigger-count 10
```

To disable next-hop-tracking status, enter the following commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp nexthop-trigger-count
```

Related commands

bgp nexthop-trigger delay

bgp nexthop-trigger enable

show bgp nexthop-tracking (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp nexthop-trigger delay

Overview Use this command to set the delay interval for next hop address tracking.

Use the **no** variant of this command to reset the timer value to the default.

Syntax

```
bgp nexthop-trigger delay <1-100>
no bgp nexthop-trigger delay
```

Parameter	Description
<1-100>	Next hop trigger delay interval in seconds.

Default The default next hop delay interval is 5 seconds.

Mode Global Configuration

Usage This command configures the delay interval between routing table waits for next hop delay tracking. The delay interval determines how long BGP waits after it receives the trigger from the system about one or more next hop changes before it walks the full BGP table to determine which prefixes are affected by the next hop changes.

Example To set the next hop delay interval to 6 seconds, enter the command:

```
awplus# configure terminal
awplus(config)# bgp nexthop-trigger delay 6
```

Related commands bgp nexthop-trigger-count

bgp nexthop-trigger enable

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp nexthop-trigger enable

Overview Use this command to enable next hop address tracking. If next hop address tracking is enabled and a next hop trigger delay interval has not been explicitly set with the bgp nexthop-trigger delay command, the default delay interval of 5 seconds is used.

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

Syntax
```
bgp nexthop-trigger enable
no bgp nexthop-trigger enable
```

Default Disabled.

Mode Global Configuration

Usage Next hop address tracking is an event driven notification system that monitors the status of routes installed in the Routing Information Base (RIB) and reports next hop changes that affect internal BGP (iBGP) or external BGP (eBGP) prefixes directly to the BGP process. This improves the overall BGP convergence time, by allowing BGP to respond rapidly to next hop changes for routes installed in the RIB.

If next hop tracking is enabled after certain routes are learned, the registration of all the next hops of selected BGP routes are done immediately after the next hop tracking feature is enabled.

If next hop tracking is disabled, and if there are still some selected BGP routes, BGP deregisters the next hops of all of the selected BGP routes from the system.

If next hop tracking is disabled when next hop tracking is in the process of execution, an error appears, and next hop tracking is not disabled. However, if the next hop tracking timer is running at the time of negation, the next hop tracking timer is stopped, and next hop tracking is disabled.

Example To enable next hop address tracking, enter the command:

```
awplus# configure terminal
awplus(config)# bgp nexthop-trigger enable
```

Related commands

bgp nexthop-trigger-count

bgp nexthop-trigger delay

show bgp nexthop-tracking (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp rfc1771-path-select (BGP only)

Overview Use this command to set the RFC1771 compatible path selection mechanism.

Use the **no** variant of this command to revert this setting.

Syntax

```
bgp rfc1771-path-select
no bgp rfc1771-path-select
```

Default Industry standard compatible path selection mechanism.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# bgp rfc1771-path-select
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp rfc1771-strict (BGP only)

Overview Use this command to set the Strict RFC1771 setting.

Use the **no** variant of this command to revert this setting.

Syntax

```
bgp rfc1771-strict
no bgp rfc1771-strict
```

Default Disabled

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# bgp rfc1771-strict
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp router-id

Overview Use this command to configure the router identifier. The IPv4 address specified in this command does not have to be an IPv4 address that is configured on any of the interfaces on the device. Note that you must specify an IPv4 address with this when used for BGP4+.

Use the **no** variant of this command to return the router-id to its default value (as described in Default below).

Syntax

```
bgp router-id <routerid>
no bgp router-id [<routerid>]
```

Parameter	Description
<routerid>	Specify the IPv4 address without mask for a manually configured router ID, in the format `A.B.C.D`.

Default If the BGP router ID is not specified, the IPv4 address of the loopback interface is used. When there is no address on the loopback interface, the highest IP address among the VLAN interfaces is used.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Usage Use the **bgp router-id** command to manually configure a fixed router ID as a BGP or BGP4+ router identifier. This router ID takes precedence over all other possible router ID sources. The order of precedence is:

1) router ID configured with this command
2) IP address of the loopback interface
3) highest IP address from the VLAN interfaces

Examples To configure a router ID with an IPv4 address for a BGP or BGP4+ router identifier, enter the commands listed below:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp router-id 1.1.2.3
```

To disable the router ID for a BGP or BGP4+ router identifier enter the commands listed below:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp router-id
```

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp scan-time (BGP only)

Overview Use this command to set the interval for BGP route next-hop scanning.

Use the **no** variant of this command to disable this function.

Syntax

```
bgp scan-time <time>
no bgp scan-time [<time>]
```

Parameter	Description
<time>	<0-60> Scanning interval in seconds.

Default The default scanning interval is 60 seconds.

Mode Router Configuration

Usage Use this command to configure scanning intervals of BGP routers. This interval is the period after which router checks the validity of the routes in its database.

To disable BGP scanning, set the scan time interval to 0 seconds.

Example

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp scan-time 10
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp update-delay

Overview Use this command to specify the update-delay value for a graceful-restart capable router.

Use the **no** variant of this command to revert to the default update-delay value.

Syntax

```
bgp update-delay <1-3600>
no bgp update-delay [<1-3600>]
```

Parameter	Description
<1-3600>	Delay value in seconds.

Default The default update-delay value is 120 seconds.

Mode Router Configuration

Usage The update-delay value is the maximum time a graceful-restart capable router which is restarting will defer route-selection and advertisements to all its graceful-restart capable neighbors. This maximum time starts from the instance the first neighbor attains established state after restart. The restarting router prematurely terminates this timer when end-of-rib markers are received from all its graceful-restart capable neighbors.

Example

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# bgp update-delay 345
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear bgp *

Overview Use this command to reset the BGP and BGP4+ connections for all peers.

Syntax

```
clear bgp *
clear bgp * in [prefix-filter]
clear bgp * out
clear bgp * soft [in|out]
```

Parameter	Description
`*`	Clears all BGP and BGP4+ peers.
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples

```
awplus# clear bgp * soft in
awplus# clear bgp * in prefix-filter
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear bgp (IPv4 or IPv6 address)

Overview Use this command to reset the BGP and BGP4+ connections for specified peers.

Syntax [BGP]

```
clear bgp <ip-addr>
clear bgp <ip-addr> in [prefix-filter]
clear bgp <ip-addr> out
clear bgp <ip-addr> soft [in|out]
```

Syntax [BGP4+]

```
clear bgp <ipv6-addr>
clear bgp <ipv6-addr> in [prefix-filter]
clear bgp <ipv6-addr> out
clear bgp <ipv6-addr> soft [in|out]
```

Parameter	Description
<ip-addr>	Specifies the IPv4 address of the neighbor whose connection is to be reset, entered in the form A.B.C.D.
<ipv6-addr>	Specifies the IPv6 address of the neighbor whose connection is to be reset, entered in hexadecimal in the format X:X::X:X.
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples [BGP]

```
awplus# clear bgp 3.3.3.3 soft in prefix-filter
awplus# clear bgp 2.2.2.2 out
```

Examples [BGP4+]

```
awplus# clear bgp 2001:0db8:010d::1 soft in prefix-filter
awplus# clear bgp 2001:0db8:010d::1 out
```

Related commands

clear bgp (IPv4 or IPv6 address)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear bgp (ASN)

Overview Use this command to reset the BGP and BGP4+ connections for peers in the specified Autonomous System Number (ASN).

Syntax

```
clear bgp <asn> [in [prefix-filter]|out|soft [in|out]]
```

Parameter	Description
`<asn>`	`<1-4294967295>` The AS Number for which all routes will be cleared.
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples

```
awplus# clear bgp 300 soft in prefix-filter
awplus# clear bgp 500 soft out
awplus# clear bgp 300 soft in
awplus# clear bgp 1 in prefix-filter
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear bgp external

Overview Use this command to reset the BGP and BGP4+ connections for all external peers.

Syntax

```
clear bgp external [in [prefix-filter]|out|soft [in|out]]
```

Parameter	Description
`external`	Clears all external peers.
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples

```
awplus# clear bgp external soft in
awplus# clear bgp external in prefix-filter
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear bgp peer-group

Overview Use this command to reset the BGP and BGP4+ connections for all members of a peer group.

Syntax

```
clear bgp peer-group <peer-group> [in [prefix-filter]|out|soft [in|out]]
```

Parameter	Description
`peer-group`	Clears all members of a peer group.
<peer-group>	Name of the BGP peer group
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples

```
awplus# clear bgp peer-group P1 soft in
awplus# clear bgp peer-group P2 in
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear bgp ipv6 (ipv6 address) (BGP4+ only)

Overview Use this command to reset the IPv6 BGP4+ connection to the peer specified by the IP address.

Syntax

```
clear bgp ipv6 <ipv6-addr> [in [prefix-filter]|out|soft
[in|out]]
```

Parameter	Description
<ipv6-addr>	Specifies the IPv6 address of the neighbor whose connection is to be reset, entered in hexadecimal in the format X:X::X:X.
ipv6	Clears all IPv6 address family peers. Configure parameters relating to the BGP4+ exchange of IPv6 prefixes.
in	Indicates that incoming advertised routes will be cleared.
prefix-filter	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
out	Indicates that outgoing advertised routes will be cleared.
soft in	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
soft out	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples Use the following command to clear the BGP4+ connection to peer at IPv6 address 2001:0db8:010d::1, and clearing all incoming routes.

```
awplus# clear ip bgp 2001:0db8:010d::1 in
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear bgp ipv6 dampening (BGP4+ only)

Overview Use this command to clear route dampening information and unsuppress routes that have been suppressed routes.

Syntax

```
clear bgp ipv6 dampening
[<ipv6-addr>|<ipv6-addr/prefix-length>]
```

Parameter	Description
<ipv6-addr>	Specifies the IPv6 address for which BGP4+ dampening is to be cleared, entered in hexadecimal in the format X:X::X:X.
<ipv6-addr/prefix-length>	Specifies the IPv6 address and prefix-length for which BGP4+ dampening is to be cleared. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.

Mode Privileged Exec

Examples

```
awplus# clear bgp ipv6 dampening 2001:0db8:010d::1
awplus# clear bgp ipv6 dampening 2001:0db8::/64
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear bgp ipv6 flap-statistics (BGP4+ only)

Overview Use this command to clear the flap count and history duration for the specified prefixes.

Syntax

```
clear bgp ipv6 flap-statistics
[<ipv6-addr>|<ipv6-addr/prefix-length>]
```

Parameter	Description
<ipv6-addr>	Specifies the IPv6 address for which BGP4+ flap count and history duration are to be cleared, entered in hexadecimal in the format X:X::X:X.
<ipv6-addr/prefix-length>	Specifies the IPv6 address with prefix length for which BGP4+ flap count and history duration are to be cleared. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.

Mode Privileged Exec

Examples

```
awplus# clear bgp ipv6 flap-statistics 2001:0db8:010d::1
awplus# clear bgp ipv6 flap-statistics 2001:0db8::/64
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear bgp ipv6 (ASN) (BGP4+ only)

Overview Use this command to reset the BGP4+ connections to all peers in a specified Autonomous System Number (ASN).

Syntax

```
clear bgp ipv6 <asn> [in [prefix-filter]|out|soft [in|out]]
clear bgp ipv6 <asn>
clear bgp ipv6 <asn> in [prefix-filter]
clear bgp ipv6 <asn> out
clear bgp ipv6 <asn> soft [in|out]
```

Parameter	Description
<asn>	<1-4294967295> Specifies the ASN for which all routes will be cleared.
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples

```
awplus# clear bgp ipv6 100
awplus# clear bgp ipv6 100 in
awplus# clear bgp ipv6 100 in prefix-filter
awplus# clear bgp ipv6 100 out
awplus# clear bgp ipv6 100 soft out
awplus# clear bgp ipv6 100 soft in
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear bgp ipv6 external (BGP4+ only)

Overview Use this command to reset the BGP4+ connections to all external peers.

Syntax

```
clear bgp ipv6 external [in [prefix-filter]|out|soft [in|out]]
clear bgp ipv6 external
clear bgp ipv6 external in [prefix-filter]
clear bgp ipv6 external out
clear bgp ipv6 external soft [in|out]
```

Parameter	Description
`external`	Clears all external peers.
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples

```
awplus# clear bgp ipv6 external in
awplus# clear bgp ipv6 external in prefix
awplus# clear bgp ipv6 external out
awplus# clear bgp ipv6 external soft out
awplus# clear bgp ipv6 external soft in
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear bgp ipv6 peer-group (BGP4+ only)

Overview Use this command to reset the BGP4+ connections to all members of a peer group.

Syntax

```
clear bgp ipv6 peer-group <peer-name>
clear bgp ipv6 peer-group <peer-name> in [prefix-filter]
clear bgp ipv6 peer-group <peer-name> out
clear bgp ipv6 peer-group <peer-name> soft [in|out]
```

Parameter	Description
`peer-group`	Clears all members of a peer group.
<peer-name>	Specifies the name of the peer group for which all members will be cleared.
`ipv6`	Clears all IPv6 address family peers. Configure parameters relating to the BGP4+ exchange of IPv6 prefixes.
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Example

```
awplus# clear bgp ipv6 peer-group Peer1 out
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear ip bgp * (BGP only)

Overview Use this command to reset all BGP connections, either by fully resetting sessions or by performing soft resets.

Syntax

```
clear ip bgp *
clear ip bgp * in
clear ip bgp * out
clear ip bgp * soft [in|out]
clear ip bgp * in [prefix-filter]
```

Parameter	Description
`*`	Clears all BGP peers.
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples To clear all BGP peers, use the command:

```
awplus# clear ip bgp *
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear ip bgp (IPv4) (BGP only)

Overview Use this command to reset the IPv4 BGP connection to the peer specified by the IP address.

Syntax [BGP]

```
clear ip bgp <ipv4-addr> [in [prefix-filter]|out|soft [in|out]]
```

Parameter	Description
<ipv4-addr>	Specifies the IPv4 address of the neighbor whose connection is to be reset, entered in the form A.B.C.D.
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local switch, without resetting the connection or clearing the entries in the local switch. So, the local switch stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the switch to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode [BGP] Privileged Exec

Examples [BGP] To clear the BGP connection to the peer at IPv4 address 192.168.1.1 and clear all incoming routes, use the following command:

```
awplus# clear ip bgp 192.168.1.1 in
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear ip bgp dampening (BGP only)

Overview Use this command to clear route dampening information and unsuppress routes that have been suppressed.

Syntax

```
clear ip bgp dampening [<ip-address>|<ip-address/m>]
```

Parameter	Description
<ip-address>	Specifies the IPv4 address for which BGP dampening is to be cleared, in dotted decimal format.
<ip-address/m>	Specifies the IPv4 address with mask for which BGP dampening is to be cleared, entered in the form A.B.C.D/M. Where M is the subnet mask
ipv4	Clears all IPv4 address family peers. Configure parameters relating to the BGP exchange of IPv4 prefixes.

Mode Privileged Exec

Examples

```
awplus# clear ip bgp dampening 10.10.0.121
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear ip bgp flap-statistics (BGP only)

Overview Use this command to clear the flap count and history duration for the specified prefixes.

Syntax

```
clear ip bgp flap-statistics [<ip-address>|<ip-address/m>]
```

Parameter	Description
<ip-address>	Specifies the IPv4 address for which BGP flap count and history duration are to be cleared.
<ip-address/m>	Specifies the IPv4 address with mask for which BGP flap count and history duration are to be cleared.
ipv4	Clears all IPv4 address family peers. Configure parameters relating to the BGP exchange of IPv4 prefixes.

Mode Privileged Exec

Examples

```
awplus# clear ip bgp flap-statistics 10.10.0.121
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear ip bgp (ASN) (BGP only)

Overview Use this command to reset the BGP connections to all peers in a specified Autonomous System Number (ASN).

Syntax

```
clear ip bgp <asn> [in [prefix-filter]|out|soft [in|out]]
clear ip bgp <asn> ipv4
clear ip bgp <asn> ipv4 in [prefix-filter]
clear ip bgp <asn> ipv4 out
clear ip bgp <asn> ipv4 soft [in|out]
```

Parameter	Description
<asn>	<1-4294967295> Specifies the ASN for which all routes will be cleared.
ipv4	Clears all IPv4 address family peers. Configure parameters relating to the BGP exchange of IPv4 prefixes.
in	Indicates that incoming advertised routes will be cleared.
prefix-filter	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
out	Indicates that outgoing advertised routes will be cleared.
soft in	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
soft out	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples

```
awplus# clear ip bgp 100
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear ip bgp external (BGP only)

Overview Use this command to reset the BGP connections to all external peers.

Syntax

```
clear ip bgp external [in [prefix-filter]|out|soft [in|out]]
clear ip bgp external
clear ip bgp external in [prefix-filter]
clear ip bgp external out
clear ip bgp external soft [in|out]
```

Parameter	Description
`external`	Clears all external peers.
`ipv4`	Clears all IPv4 address family peers. Configure parameters relating to the BGP exchange of IPv4 prefixes.
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples

```
awplus# clear ip bgp external out
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear ip bgp peer-group (BGP only)

Overview Use this command to reset the BGP connections to all members of a peer group.

Syntax

```
clear ip bgp peer-group <peer-name>
clear ip bgp peer-group <peer-name> in [prefix-filter]
clear ip bgp peer-group <peer-name> out
clear ip bgp peer-group <peer-name> soft [in|out]
clear ip bgp peer-group <peer-name> out
clear ip bgp peer-group <peer-name> soft [in|out]
```

Parameter	Description
`peer-group`	Clears all members of a peer group.
<peer-name>	Specifies the name of the peer group for which all members will be cleared.
`ipv4`	Clears all IPv4 address family peers. Configure parameters relating to the BGP exchange of IPv4 prefixes.
`in`	Indicates that incoming advertised routes will be cleared.
`prefix-filter`	Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.
`out`	Indicates that outgoing advertised routes will be cleared.
`soft in`	Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory.
`soft out`	Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.

Mode Privileged Exec

Examples

```
awplus# clear ip bgp peer-group Peer1 out
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

clear ip prefix-list

Overview Use this command to reset the hit count to zero in the prefix-list entries.

Syntax `clear ip prefix-list [<list-name>] [<ip-address>/<mask>]`

Parameter	Description
<list-name>	The name of the prefix-list.
<ip-address>/<mask>	The IP prefix and length.

Mode Privileged Exec

Example To clear a prefix-list named List1:

```
awplus# clear ip prefix-list List1
```

debug bgp (BGP only)

Overview Use this command to turn on one or more BGP debug options.

Use the **no** variant of this command to disable one or more BGP debug options.

Syntax

```
debug bgp
[all|dampening|events|filters|fsm|keepalives|nht|nsm|updates
[in|out]]
```

```
no debug all bgp
```

```
no debug bgp
[all|dampening|events|filters|fsm|keepalives|nht|nsm|updates
[in|out]]
```

Parameter	Description
`all`	Turns on all debugging for BGP.
`dampening`	Specifies debugging for BGP dampening.
`events`	Specifies debugging for BGP events.
`filters`	Specifies debugging for BGP filters.
`fsm`	Specifies debugging for BGP Finite State Machine (FSM).
`keepalives`	Specifies debugging for BGP keepalives.
`nht`	Specifies debugging for BGP NHT (Next Hop Tracking) messages.
`nsm`	Specifies debugging for NSM messages.
`updates`	`[in|out]` Specifies debugging for BGP updates.
`in`	Inbound updates.
`out`	Outbound updates.

Mode Privileged Exec and Global Configuration

Usage If the command is entered with no parameters, then all debug options are enabled.

Examples

```
awplus# debug bgp
awplus# debug bgp events
awplus# debug bgp nht
awplus# debug bgp updates in
```

Related commands show debugging bgp (BGP only)

undebug bgp (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

distance (BGP and BGP4+)

Overview This command sets the administrative distance for BGP and BGP4+ routes. The device uses this value to select between two or more routes to the same destination from two different routing protocols. Set the administrative distance for BGP routes in the Router Configuration mode, and for BGP4+ routes in IPv6 Address Family Configuration mode.

The route with the smallest administrative distance value is added to the Forwarding Information Base (FIB). For more information, see the Route Selection Feature Overview and Configuration Guide, which is available from the above link at alliedtelesis.com.

The **no** variant of this command sets the administrative distance for the route to the default for the route type.

Syntax

```
distance <1-255> <ip-address/m> [<listname>]
distance bgp <ebgp> <ibgp> <local>
no distance <1-255> <ip-address/m> [<listname>]
no distance bgp <ebgp> <ibgp> <local>
```

Parameter	Description
<1-255>	The administrative distance value you are setting for the route.
<ip-address/m>	The IP source prefix that you are changing the administrative distance for, entered in the form `A.B.C.D/M`. This is an IPv4 address in dotted decimal notation followed by a forward slash, and then the prefix length.
<listname>	The name of the access list to be applied to the administrative distance to selected routes.
<ebgp>	Specifies the administrative distance of external BGP (eBGP) routes. These are routes learned from a neighbor out of the AS. Specify the distance as a number between 1 and 255. Default: **20**
<ibgp>	Specifies the administrative distance of internal BGP (iBGP) routes. These are routes learned from a neighbor within the same AS. Specify the distance as a number between 1 and 255. Default: **200**
<local>	Specifies the administrative distance of local BGP routes. These are routes redistributed from another protocol within your device. Specify the distance as a number between 1 and 255. Default: **200**

Mode [BGP] Router Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage notes You can use this command to set the administrative distance:

- for each BGP route type by specifying:

```
awplus(config-router)# distance <ebgp> <igbp> <local>
```

- for a specific route by specifying:

```
awplus(config-router)# distance <1-255> <ip-address/m>
[<listname>]
```

If the administrative distance is changed, it could create inconsistency in the routing table and obstruct routing.

Examples [BGP]

For BGP IPv4, to set the administrative distance to 34 for the route 10.10.0.0/24 in BGP 100, and use the access list "mylist" to filter the routes, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# distance 34 10.10.0.0/24 mylist
```

For BGP IPv4, to set BGP 100's administrative distances for eBGP routes to 34, iBGP routes to 23, and local BGP routes to 15, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# distance bgp 34 23 15
```

Example [BGP4+]

For BGP4+ IPv6, to set BGP 100's administrative distances for eBGP routes to 34, iBGP routes to 23, and local BGP routes to 15, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# distance bgp 34 23 15
```

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

exit-address-family

Overview Use this command to exit either the IPv4 or the IPv6 Address Family Configuration mode.

Syntax
```
exit-address-family
```

Mode [BGP] IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Examples [BGP] To enter and then exit IPv4 Address Family Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv4
awplus(config-router-af)# exit-address-family
awplus(config-router)#
```

Example [BGP4+] To enter and then exit IPv6 Address Family Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# exit-address-family
awplus(config-router)#
```

Related commands address-family

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

ip as-path access-list

Overview This command defines a BGP and BGP4+ Autonomous System (AS) path access list.

The named AS path list is a filter based on regular expressions. If the regular expression matches the AS path in a BGP update message, then the permit or deny condition applies to that update. Use this command to define the BGP access list globally, then use neighbor configuration commands to apply the list to a particular neighbor.

The **no** variant of this command disables the use of the access list.

Syntax

```
ip as-path access-list <listname> {deny|permit} <reg-exp>
no ip as-path access-list <listname> {deny|permit} <reg-exp>
```

Parameter	Description
`<listname>`	Specifies the name of the access list.
`deny`	Denies access to matching conditions.
`permit`	Permits access to matching conditions.
`<reg-exp>`	Specifies a regular expression to match the BGP AS paths.

Regular expressions listed below can be used with the **ip as-path-access-list** command:

Symbol	Character	Meaning
^	Caret	Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign	Used to match the end of the input string.
.	Period	Used to match a single character (white spaces included).
*	Asterisk	Used to match none or more sequences of a pattern.
+	Plus sign	Used to match one or more sequences of a pattern.
?	Question mark	Used to match none or one occurrence of a pattern.
_	Underscore	Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.
[ ]	Brackets	Specifies a range of single-characters.
-	Hyphen	Separates the end points of a range.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# ip as-path access-list mylist deny ^65535$
```

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

ip community-list

Overview Use this command to add an entry to a standard or extended BGP community-list filter.

Use the **no** variant of this command to delete a standard or extended community list entry.

Syntax

```
ip community-list <listname> {deny|permit} .<community>
no ip community-list <listname> {deny|permit} .<community>
```

Parameter	Description
<listname>	Specifies the community listname.
deny	Specifies the community to reject.
permit	Specifies the community to accept.
.*<community>*	{<AS:VAL>|local-AS|no-advertise|no-export}
<AS:VAL>	Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit format.
local-AS	Specifies routes not to be advertised to external BGP peers.
no-advertise	Specifies routes not to be advertised to other BGP peers.
no-export	Specifies routes not to be advertised outside of Autonomous System boundary.

Mode Global Configuration

Usage notes A community-list can be used as a filter to BGP updates. Use this command to define the community access list globally, then use neighbor configuration commands to apply the list to a particular neighbor.

There are two kinds of community-lists: expanded and standard. A standard community- list defines the community attributes explicitly and not via a regular expression. An expanded community-list defines the communities attributes with regular expressions.

The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value that does not match the standard community value is automatically treated as expanded.

Example

```
awplus# configure terminal
awplus(config)# ip community-list mylist permit 7675:80 7675:90
```

Related commands

ip community-list standard

ip community-list expanded

show ip community-list

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

ip community-list expanded

Overview Use this command to add an entry to an expanded BGP community-list filter.

Use the **no** variant of this command to delete the community list entry.

Syntax

```
ip community-list <100-199> {deny|permit} .<line>
no ip community-list <100-199> {deny|permit} .<line>
ip community-list expanded <expanded-listname> {deny|permit}
.<line>
no ip community-list expanded <expanded-listname> {deny|permit}
.<line>
```

Parameter	Description
<100-199>	Expanded community list number.
`expanded`	Specifies an expanded community list.
<expanded-listname>	Expanded community list entry.
`deny`	Specifies community to reject.
`permit`	Specifies community to accept.
`.`*<line>*	Specifies community attributes with regular expressions.

Regular expressions listed below can be used with the **ip community-list expanded** command:

Symbol	Character	Meaning
^	Caret	Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign	Used to match the end of the input string.
.	Period	Used to match a single character (white spaces included).
*	Asterisk	Used to match none or more sequences of a pattern.
+	Plus sign	Used to match one or more sequences of a pattern.
?	Question mark	Used to match none or one occurrence of a pattern.
_	Underscore	Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.
[ ]	Brackets	Specifies a range of single-characters.
-	Hyphen	Separates the end points of a range.

Mode Global Configuration

Usage notes A `community-list` can be used as a filter to BGP updates. Use this command to define the community access list globally, then use **neighbor** configuration commands to apply the list to a particular neighbor.

There are two kinds of community-lists: expanded and standard. A standard community- list defines the community attributes explicitly and not via a regular expression. An expanded community-list defines the communities attributes with regular expressions.

The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value that does not match the standard community value is automatically treated as expanded.

Examples

```
awplus# configure terminal
awplus(config)# ip community-list 125 permit 6789906
awplus(config)# ip community-list expanded CLIST permit .*
```

Related commands

ip community-list

ip community-list standard

show ip community-list

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

ip community-list standard

Overview Use this command to add an entry to a standard BGP community-list filter.

Use the **no** variant of this command to delete the standard community-list entry.

Syntax

```
ip community-list <1-99> {deny|permit} [.<community>]
no ip community-list <1-99> {deny|permit} [.<community>]
ip community-list standard <standard-listname> {deny|permit}
[.<community>]
no ip community-list standard <standard-listname> {deny|permit}
[.<community>]
```

Parameter	Description
<1-99>	Standard community list number.
`standard`	Specifies a standard community list.
<standard-listname>	Standard community list entry.
`deny`	Specifies community to reject.
`permit`	Specifies community to accept.
<community>	{*<AS:VAL>*| local-AS | no-advertise | no-export}
<AS:VAL>	Specifies the valid value for the community number. This format represents the 32 bit communities value, where `AS` is the high order 16 bits and `VAL` is the low order 16 bits in digit format.
`local-AS`	Specifies routes not to be advertised to external BGP peers.
`no-advertise`	Specifies routes not to be advertised to other BGP peers.
`no-export`	Specifies routes not to be advertised outside of the Autonomous System boundary.

Mode Global Configuration

Usage notes A community-list can be used as a filter to BGP updates. Use this command to define the community access list globally, then use neighbor configuration commands to apply the list to a particular neighbor.

There are two kinds of community-lists: expanded and standard. The standard community-list defines the community attributes as explicit values, without regular expressions. The expanded community-list defines the communities attributes with regular expressions.

The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value

that does not match the standard community value is automatically treated as expanded.

Examples

```
awplus# configure terminal
awplus(config)# ip community-list standard CLIST permit 7675:80
7675:90 no-export
awplus(config)# ip community-list 34 permit 5675:50
no-advertise
```

Related commands

ip community-list

ip community-list expanded

show ip community-list

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

ip extcommunity-list expanded

Overview Use this command to create or delete an expanded extended community list.

Use the **no** variant of this command to delete the expanded extended community-list entry.

Syntax

```
ip extcommunity-list <100-199> {deny|permit}
{.<line>|.<AS:NN>|.<ip-address>}

no ip extcommunity-list <100-199> {deny|permit}
{.<line>|.<AS:NN>|.<ip-address>}

ip extcommunity-list expanded <expanded-listname> {deny|permit}
{.<line>|.<AS:NN>|.<ip-address>}

no ip extcommunity-list expanded <expanded-listname>
{deny|permit} {.<line>|.<AS:NN>|.<ip-address>}

no ip extcommunity-list <100-199>

no ip extcommunity-list expanded <expanded-listname>
```

Parameter	Description
<100-199>	Expanded extcommunity list number.
expanded	Specifies an expanded extcommunity list.
<expanded-listname>	Expanded extcommunity list entry.
deny	Specifies the extcommunity to reject.
permit	Specifies the extcommunity to accept.
.<line>	Specifies extcommunity attributes with regular expression.
<AS:NN>	Specifies the valid value for an extcommunity number. This format represents the 32 bit extcommunities value, where AA is the high order 16 bits and NN is the low order 16 bits in digit format.
<ip-address>	Specifies the IP address to deny or permit.

Regular expressions listed below are used with the **ip extcommunity-list expanded** command:

Symbol	Character	Meaning
^	Caret	Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign	Used to match the end of the input string.

Symbol	Character	Meaning
.	Period	Used to match a single character (white spaces included).
*	Asterisk	Used to match none or more sequences of a pattern.
+	Plus sign	Used to match one or more sequences of a pattern.
?	Question mark	Used to match none or one occurrence of a pattern.
_	Underscore	Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.
[ ]	Brackets	Specifies a range of single-characters.
-	Hyphen	Separates the end points of a range.

Mode Global Configuration

Examples

```
awplus# configure terminal
awplus(config)# ip extcommunity-list 125 permit 4567335
awplus(config)# ip extcommunity-list expanded CLIST permit .*
```

Related commands ip extcommunity-list standard

show ip extcommunity-list

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

ip extcommunity-list standard

Overview Use this command to create and delete a standard extended community list.

Use the **no** variant of this command to delete a standard extended community-list entry.

Syntax

```
ip extcommunity-list <1-99> {deny|permit} {rt|soo}
<community-number>
```

```
ip extcommunity-list standard <standard-listname> {deny|permit}
{rt|soo} <community-number>
```

```
no ip extcommunity-list <1-99> [{deny|permit} {rt|soo}
<community-number>]
```

```
no ip extcommunity-list standard <standard-listname>
[{deny|permit} {rt|soo} <community-number>]
```

Parameter	Description
<1-99>	Standard extcommunity list number.
standard	Specifies a standard extended community list.
<standard-listname>	Standard extended community list entry.
deny	Specifies the extended community to reject.
permit	Specifies the extended community to accept.
rt	Specifies the route target of the extended community.
soo	Specifies the site of origin of the extended community.
<community-number>	Specifies the valid value for an extended community number. This can be one of two formats: • <ASN:NN> where *ASN* is an AS (Autonomous System) number and *NN* is a value chosen by the ASN administrator • <A.B.C.D:NN> where *A.B.C.D* is an IPv4 address, and *NN* is a value chosen by the ASN administrator. Note that *ASN* and *NN* are both integers from 1 to 4294967295. AS numbers are assigned to the regional registries by IANA (www.iana.org) and must be obtained in your region.

Mode Global Configuration

Examples

```
awplus# configure terminal
awplus(config)# ip extcommunity-list 36 permit rt 5675:50
awplus(config)# ip extcommunity-list standard CLIST permit soo 7645:70
awplus# configure terminal
awplus(config)# ip extcommunity-list 36 deny rt 192.168.1.1:70
awplus(config)# ip extcommunity-list standard CLIST deny soo 10.10.1.1:50
```

Related commands

ip extcommunity-list expanded

show ip extcommunity-list

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

ip prefix-list

Overview Use this command to create an entry for an IPv4 prefix list.

Use the **no** variant of this command to delete the IPv4 prefix-list entry.

Syntax

```
ip prefix-list <list-name> [seq <1-429496725>] {deny|permit}
{any|<ip-prefix>} [ge <0-32>] [le <0-32>]
ip prefix-list <list-name> description <text>
ip prefix-list sequence-number
no ip prefix-list <list-name> [seq <1-429496725>]
no ip prefix-list <list-name> [description <text>]
no ip prefix-list sequence-number
```

Parameter	Description
<list-name>	Specifies the name of a prefix list.
seq *<1-429496725>*	Sequence number of the prefix list entry.
deny	Specifies that the prefixes are excluded from the list.
permit	Specifies that the prefixes are included in the list.
<ip-prefix>	Specifies the IPv4 address and length of the network mask in dotted decimal in the format A.B.C.D/M.
any	Any prefix match. Same as **0.0.0.0/0 le 32**.
ge*<0-32>*	Specifies the minimum prefix length to be matched.
le*<0-32>*	Specifies the maximum prefix length to be matched.
<text>	Text description of the prefix list.
sequence-number	Specify sequence numbers included or excluded in prefix list.

Mode Global Configuration

Usage notes When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the **seq** parameter and place common permits or denials towards the top of the list. If you do not use the **seq** parameter, the sequence values are generated in a sequence of 5.

The parameters **ge** and **le** specify the range of the prefix lengths to be matched. When setting these parameters, set the **le** value to be less than 32, and the **ge** value to be less than or equal to the **le** value and greater than the ip-prefix mask length.

Prefix lists implicitly exclude prefixes that are not explicitly permitted in the prefix list. This means if a prefix that is being checked against the prefix list reaches the end of the prefix list without matching a permit or deny, this prefix will be denied.

Example In the following sample configuration, the last **ip prefix-list** command in the below list matches all, and the first **ip prefix-list** command denies the IP network 76.2.2.0:

```
awplus(config)# router bgp 100
awplus(config-router)# network 172.1.1.0
awplus(config-router)# network 172.1.2.0
awplus(config-router)# neighbor 10.6.5.3 remote-as 300
awplus(config-router)# neighbor 10.6.5.3 prefix-list mylist out
awplus(config-router)# exit
awplus(config)# ip prefix-list mylist seq 5 deny 76.2.2.0/24
awplus(config)# ip prefix-list mylist seq 100 permit any
```

To deny the IP addresses between 10.0.0.0/14 (10.0.0.0 255.252.0.0) and 10.0.0.0/22 (10.0.0.0 255.255.252.0) within the 10.0.0.0/8 (10.0.0.0 255.0.0.0) addressing range, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip prefix-list mylist seq 12345 deny 10.0.0.0/8
ge 14 le 22
```

Related commands

match ip address

neighbor prefix-list

area filter-list

clear ip prefix-list

match route-type

show ip prefix-list

ipv6 prefix-list

Overview Use this command to create an IPv6 prefix list or an entry in an existing prefix list.

Use the **no** variant of this command to delete a whole prefix list, a prefix list entry, or a description.

Syntax

```
ipv6 prefix-list <list-name> [seq <1-429496725>] {deny|permit} {any|<ipv6-prefix>} [ge <0-128>] [le <0-128>]
ipv6 prefix-list <list-name> description <text>
no ipv6 prefix-list <list-name> [seq <1-429496725>]
no ipv6 prefix-list <list-name> [description <text>]
```

Parameter	Description
`<list-name>`	Specifies the name of a prefix list.
`seq <1-429496725>`	Sequence number of the prefix list entry.
`deny`	Specifies that the prefixes are excluded from the list.
`permit`	Specifies that the prefixes are included in the list.
`<ipv6-prefix>`	Specifies the IPv6 prefix and prefix length in hexadecimal in the format X:X::X:X/M.
`any`	Any prefix match. Same as ::0/0 le 128.
`ge <0-128>`	Specifies the minimum prefix length to be matched.
`le <0-128>`	Specifies the maximum prefix length to be matched.
`description`	Prefix list specific description.
`<text>`	Up to 80 characters of text description of the prefix list.

Mode Global Configuration

Usage notes When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the **seq** parameter and place common permits or denials towards the top of the list. If you do not use the **seq** parameter, the sequence values are generated in a sequence of 5.

The parameters **ge** and **le** specify the range of the prefix lengths to be matched. The parameters **ge** and **le** are only used if an ip-prefix is stated. When setting these parameters, set the **le** value to be less than 128, and the **ge** value to be less than or equal to the **le** value and greater than the ip-prefix mask length.

Prefix lists implicitly exclude prefixes that are not explicitly permitted in the prefix list. This means if a prefix that is being checked against the prefix list reaches the end of the prefix list without matching a permit or deny, this prefix will be denied.

Example To check the first 32 bits of the prefix 2001:db8:: and that the subnet mask must be greater than or equal to 34 and less than or equal to 40, enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 prefix-list mylist seq 12345 permit
2001:db8::/32 ge 34 le 40
```

Related commands

match ipv6 address

show ipv6 prefix-list

show running-config ipv6 prefix-list

match as-path

Overview Use this command to add an autonomous system (AS) path match clause to a route map entry. Specify the AS path attribute value or values to match by specifying the name of an AS path access list. To create the AS path access list, enter Global Configuration mode and use the ip as-path access-list command.

A BGP update message matches the route map if its attributes include AS path values that match the AS path access list.

Each entry of a route map can only match against one AS path access list in one AS path match clause. If the route map entry already has an AS path match clause, entering this command replaces that match clause with the new clause.

Note that AS path access lists and route map entries both specify an action of deny or permit. The action in the AS path access list determines whether the route map checks update messages for a given AS path value. The route map action and its **set** clauses determine what the route map does with update messages that contain that AS path value.

Use the **no** variant of this command to remove the AS path match clause from a route map entry.

Syntax

```
match as-path <as-path-listname>
no match as-path [<as-path-listname>]
```

Parameter	Description
<as-path-listname>	Specifies an AS path access list name.

Mode Route-map Configuration

Usage notes This command is valid for BGP update messages only.

Example To add entry `34` to the route map called `myroute`, which will discard update messages if they contain the AS path values that are included in `myaccesslist`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute deny 34
awplus(config-route-map)# match as-path myaccesslist
```

Related commands route-map

set as-path

show route-map

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

match community

Overview Use this command to add a community match clause to a route map entry. Specify the community value or values to match by specifying a community list. To create the community list, enter Global Configuration mode and use the ip community-list command.

A BGP update message matches the route map if its attributes include community values that match the community list.

Each entry of a route map can only match against one community list in one community match clause. If the route map entry already has a community match clause, entering this command replaces that match clause with the new clause.

Note that community lists and route map entries both specify an action of deny or permit. The action in the community list determines whether the route map checks update messages for a given community value. The route map action and its **set** clauses determine what the route map does with update messages that contain that community value.

Use the **no** variant of this command to remove the community match clause from a route map.

Syntax

```
match community
{<community-listname>|<1-99>|<100-199>}[exact-match]
```

```
no match community
[<community-listname>|<1-99>|<100-199>|exact-match]
```

Parameter	Description
<community-listname>	The community list name or number.
<1-99>	Community list number (standard range).
<100-199>	Community list number (expanded range).
exact-match	Exact matching of communities.

Mode Route-map Configuration

Usage notes This command is valid for BGP update messages only.

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes.

Example To add entry `3` to the route map called `myroute`, which will process update messages if they contain the community values that are included in `mylist`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# match community mylist
```

Related commands

ip community-list

route-map

set comm-list delete

set community

show route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

max-paths

Overview Use this command to set the number of equal-cost multi-path (ECMP) routes for eBGP or iBGP. You can install multiple BGP paths to the same destination to balance the load on the forwarding path.

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

Syntax

```
max-paths {ebgp|ibgp} <2-64>
no max-paths ebgp [<2-64>]
no max-paths ibgp [<2-64>]
```

Parameter	Description
ebgp	eBGP ECMP session.
ibgp	iBGP ECMP session.
<2-64>	Specifies the number of routes.

Mode Global Configuration

Usage notes This command is available for the default BGP instance and for IPV4 and IPv6 unicast addresses.

Example

```
awplus# configure terminal
awplus(config)# router bgp 64501
awplus(config-router)# max-paths ebgp 2
```

Related commands show ip route summary

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor activate

Overview Use this command to enable the exchange of BGP IPv4 and BGP4+ IPv6 routes with a neighboring router, and also within either an IPv4 or an IPv6 specific address-family.

Use the **no** variant of this command to disable the exchange of information with a BGP or BGP4+ neighbor, in the Router Configuration or the Address Family Configuration mode.

Syntax

```
neighbor <neighborid> activate
no neighbor <neighborid> activate
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage [BGP] Use this command to enable the exchange of information to a neighbor. To exchange IPv4 or IPv6 prefixes with a BGP or a BGP4+ peer, you must configure this command for the peer or the peer group. This command only enables the exchange of information. You can establish peering without this command, but no prefixes and other information is sent until you apply this command to the neighbor.

This command triggers the device to start a BGP or BGP4+ peering relationship with the specified BGP or BGP4+ neighbor and start exchanging routes with that neighbor.

Examples [BGP] To enable an exchange of routes with a neighboring router with the IPv4 address 10.10.10.1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 activate
```

To disable an exchange of routes with a neighboring router with the IPv4 address 10.10.10.1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 activate
```

To enable an exchange of routes in Address Family Configuration mode with a neighboring router with the IPv4 address 10.10.10.1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.1 activate
```

To disable an exchange of routes in Address Family Configuration mode with a neighboring router with the IPv4 address 10.10.10.1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.1 activate
```

To enable an exchange of routes with a neighboring router with the peer-group named group1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.63 remote-as 10
awplus(config-router)# neighbor 10.10.0.63 peer-group group1
awplus(config-router)# neighbor group1 activate
```

To disable an exchange of routes with a neighboring router with the peer-group named group1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 activate
```

Examples [BGP4+]

To enable an exchange of routes in IPv6 Address Family Configuration mode with a neighboring router with the IPv6 address 2001:0db8:010d::1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1 activate
```

To disable an exchange of routes in IPv6 Address Family Configuration mode with a neighboring router with the IPv6 address 2001:0db8:010d::1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
activate
```

To enable an exchange of routes with a neighboring router with the peer-group named group1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 activate
```

To disable an exchange of routes with a neighboring router with the peer-group named group1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 activate
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor advertisement-interval

Overview Use this command to set the minimum interval between sending iBGP or eBGP routing updates for a given route. This command reduces the flapping of individual routes.

Use the **no** variant of this command to set the interval time to the default values (30 seconds for eBGP peers and 5 seconds for iBGP peers) for a given route.

Syntax

```
neighbor <neighborid> advertisement-interval <time>
no neighbor <neighborid> advertisement-interval [<time>]
```

Parameter	Description	
<neighborid>	{*<ip-address>* | *<ipv6-addr>* | *<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group. Note that if you apply an advertisement-interval value to a peer group it will apply to all members in the peer group.
<time>	*<0-600>*	Advertisement -interval value in seconds.

Default The default interval between sending routing updates for a given route to eBGP peers is 30 seconds, and the default interval for a given route to iBGP peers is 5 seconds.

Mode Router Configuration

Usage notes Use this command to set the minimum interval between sending iBGP or eBGP routing updates for a given route. To reduce the flapping of routes to the internet, set a minimum advertisement interval, so iBGP or eBGP routing updates are sent per interval seconds.

BGP dampening can also be used to control the effects of flapping routes. See the bgp dampening command in this chapter, and the Routing_Protocol Guide for more information.

The advertisement-interval time value is the minimum time between the advertisement of Update messages sent from a BGP speaker to report changes to

eBGP or iBGP peers. This is the minimum time between two Update messages sent to iBGP or eBGP peers.

See the neighbor as-origination-interval command to set the interval time between messages to iBGP peers, which have prefixes within the local AS. Use this command instead of the neighbor as-origination-interval command for eBGP peers with prefixes not in the same AS and updates not in a local AS.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.3
advertisement-interval 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.3
advertisement-interval
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.3 remote-as 10
awplus(config-router)# neighbor 10.10.0.3 peer-group group1
awplus(config-router)# neighbor group1 advertisement-interval
45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1
advertisement-interval
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
advertisement-interval 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
advertisement-interval
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1
advertisement-interval 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1
advertisement-interval
```

Related commands

neighbor as-origination-interval

neighbor peer-group (add a neighbor)

neighbor route-map

show bgp ipv6 neighbors (BGP4+ only)

show ip bgp neighbors (BGP only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor allowas-in

Overview Use this command to accept an AS_PATH with the specified Autonomous System (AS) number from inbound updates for both BGP and BGP4+ routes.

This command allows BGP and BGP4+ to accept prefixes with the same ASN in the AS_PATH attribute. This command allows BGP and BGP4+ to accept up to 10 instances, configured by the <*occurrences*> placeholder, of its own AN in the AS_PATH for a prefix.

Use the **no** variant of this command to revert to default functionality (disabled by default).

Syntax

```
neighbor <neighborid> allowas-in <occurrences>
no neighbor <neighborid> allowas-in
```

Parameter	Description	
<*neighborid*>	{<*ip-address*>|<*ipv6-addr*>|<*peer-group*>}	
	<*ip-address*>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<*ipv6-addr*>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<*peer-group*>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<*occurrences*>	<*1-10*> Specifies the number of occurrences of the AS number.	

Default Disabled

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage Use this command to configure PE (Provider Edge) routers to allow re-advertisement of all prefixes containing duplicate Autonomous System Numbers (ASNs). In a hub and spoke configuration, a PE router re-advertises all prefixes containing duplicate ASNs. Specify the remote-as or peer-group first using the related commands. The command allows a receiving peer to accept prefixes with its own AN in the AS_PATH, up the maximum number of instances, as configured by the <*occurrences*> placeholder.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.1 allowas-in 3
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.0.1 allowas-in 3
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.1 allowas-in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.0.1 allowas-in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.1 remote-as 10
awplus(config-router)# neighbor 10.10.0.1 peer-group group1
awplus(config-router)# neighbor group1 allowas-in 3
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor group1 allowas-in 3
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
allowas-in 3
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
allowas-in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 allowas-in 3
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor group1 allowas-in 3
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor as-origination-interval

Overview Use this command to adjust the sending of AS (Autonomous System) origination routing updates to a specified iBGP peer. This command adjusts the rate at which updates are sent to a specified iBGP peer (15 seconds by default). You must set a rate when you enable it.

The as-origination-interval is the minimum time set between the advertisement of Update messages sent from a BGP speaker to an iBGP peer to report changes within the local AS.

Use the **no** variant of this command to reset the timer to the default value of 15 seconds.

Syntax [BGP]

```
neighbor <neighbor_address> as-origination-interval <time>
no neighbor <neighbor_address> as-origination-interval [<time>]
```

Syntax [BGP4+]

```
neighbor <ipv6-addr> as-origination-interval <time>
no neighbor <ipv6-addr> as-origination-interval [<time>]
```

Parameter	Description
<neighbor_address>	Specify a neighbor IPv4 address, in dotted decimal in the format A.B.C.D.
<ipv6-addr>	Specify an address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
<time>	<1-600> Time in seconds.

Default The default interval between sending routing updates to iBGP peers, which include a prefix that originates from the local AS, is 15 seconds by default.

Mode Router Configuration

Usage This command is used to change the minimum interval between sending AS-origination routing updates. The update interval for iBGP peers can be set from 1 to 600 seconds.

For interoperability with other vendors' devices, we recommend using the default value. The AS origination interval timer may not be available to adjust on other vendors' devices. Applying the default of 15 seconds across the AS maintains a common timer policy.

AlliedWare Plus devices use the default 15 second AS Origination Interval timer as per RFC 4271, a 30 second keepalive timer, a 90 second hold timer, a 120 second connect timer, a 5 second iBGP peer route advertisement interval, and a 30 second eBGP peer route advertisement interval.

Cisco devices use a 60 second keepalive timer, a 180 second hold timer, and no iBGP peer route interval timer (0). Juniper devices use a 10 second AS Origination Interval timer.

The as-origination-interval time value is the minimum amount of time between the advertisement of Update messages sent from a BGP speaker to report changes within the local AS. This is the minimum time between two Update messages to iBGP peers, which contain a prefix that originates from the same AS. See the neighbor advertisement-interval command to set time between messages to eBGP peers.

Use this command instead of the neighbor advertisement-interval command for iBGP peers with prefixes in the same AS for updates only within a local AS.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# neighbor 10.10.0.1
as-origination-interval 10
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no neighbor 10.10.0.1
as-origination-interval
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# neighbor 2001:0db8:010d::1
as-origination-interval 10
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no neighbor 2001:0db8:010d::1
as-origination-interval
```

Validation Commands

show bgp ipv6 neighbors (BGP4+ only)

show ip bgp neighbors (BGP only)

Related commands

neighbor advertisement-interval

address-family

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor attribute-unchanged

Overview Use this command to advertise unchanged BGP or BGP4+ attributes to the specified BGP or BGP4+ neighbor.

Use the **no** variant of this command to disable this function.

Syntax

```
neighbor <neighborid> attribute-unchanged
{as-path|next-hop|med}
```

```
no neighbor <neighborid> attribute-unchanged
{as-path|next-hop|med}
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*ipv6-addr*>|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
as-path	AS path attribute.	
next-hop	Next hop attribute.	
med	Multi Exit Discriminator.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage notes Note that specifying this command with the optional **as-path** parameter has the same effect as invoking the neighbor transparent-as command.

Note this specifying this command with the optional **next-hop** parameter has the same effect as invoking the neighbor transparent-nexthop command.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.75 attribute-unchanged
as-path med
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.75
attribute-unchanged as-path med
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.0.75
attribute-unchanged as-path med
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.0.75
attribute-unchanged as-path med
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.75 remote-as 10
awplus(config-router)# neighbor 10.10.0.75 peer-group group1
awplus(config-router)# neighbor group1 attribute-unchanged
as-path med
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 attribute-unchanged
as-path med
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
attribute-unchanged as-path med
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
attribute-unchanged as-path med
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 attribute-unchanged
as-path med
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1
attribute-unchanged as-path med
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

neighbor transparent-as

neighbor transparent-nexthop

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor capability graceful-restart

Overview Use this command to configure the device to advertise the Graceful Restart Capability to BGP and BGP4+ neighbors.

Use the **no** variant of this command to configure the device so it does not advertise the Graceful Restart Capability to its neighbor.

Syntax

```
neighbor <neighborid> capability graceful-restart
no neighbor <neighborid> capability graceful-restart
```

Parameter	Description	
<neighborid>	{*<ip-address>* | *<ipv6-addr>* | *<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Default Disabled

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage Use the **neighbor capability graceful-restart** command to advertise to the BGP or BGP4+ neighbor routers the capability of graceful restart. First specify the BGP or BGP4+ neighbor's **remote-as** identification number as assigned by the neighbor router.

The graceful restart capability is advertised only when the graceful restart capability has been enabled using the bgp graceful-restart command.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.50 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.50 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.50 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.50 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.50 remote-as 10
awplus(config-router)# neighbor 10.10.10.50 peer-group group1
awplus(config-router)# neighbor group1 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 capability
graceful-restart
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
capability graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
capability graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 capability
graceful-restart
```

Related commands

bgp graceful-restart

neighbor peer-group (add a neighbor)

neighbor route-map

restart bgp graceful (BGP only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor capability orf prefix-list

Overview Use this command to advertise ORF (Outbound Route Filters) capability to neighbors. Use this command to dynamically filter updates. The BGP speaker can advertise a prefix list with prefixes it wishes the peer to prune or filter from outgoing updates.

Use the **no** variant of this command to disable this function.

Syntax

```
neighbor <neighborid> capability orf prefix-list
{both|receive|send}
```

```
no neighbor <neighborid> capability orf prefix-list
{both|receive|send}
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
`orf`	Advertises ORF capability to its neighbors.	
`both`	Indicates that the local router can send ORF entries to its peer as well as receive ORF entries from its peer.	
`receive`	Indicates that the local router is willing to receive ORF entries from its peer.	
`send`	Indicates that the local router is willing to send ORF entries to its peer.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Default Disabled

Usage notes Outbound Route Filters (ORFs) send and receive capabilities to lessen the number of updates exchanged between neighbors. By filtering updates, this option minimizes generating and processing of updates. The local router advertises the ORF capability in `send` mode and the remote router receives the ORF capability in

receive mode applying the filter as outbound policy. The two routers exchange updates to maintain the ORF for each router. Only an individual router or a peer-group can be configured to be in **receive** or **send** mode. A peer-group member cannot be configured in **receive** or **send** mode.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.5 capability orf
prefix-list both
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.5 capability orf
prefix-list both
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router)# neighbor 10.10.0.5 capability orf
prefix-list both
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router)# no neighbor 10.10.0.5 capability orf
prefix-list both
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.5 remote-as 10
awplus(config-router)# neighbor 10.10.0.5 peer-group group1
awplus(config-router)# neighbor group1 capability orf
prefix-list both
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 capability orf
prefix-list both
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router)# neighbor 2001:0db8:010d::1 capability
orf prefix-list both
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router)# no neighbor 2001:0db8:010d::1 capability
orf prefix-list both
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 capability orf
prefix-list both
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 capability orf
prefix-list both
```

Related commands

neighbor capability orf prefix-list

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor capability route-refresh

Overview Use this command to advertise route-refresh capability to the specified BGP and BGP4+ neighbors.

Use the **no** variant of this command to disable this function

Syntax

```
neighbor <neighborid> capability route-refresh
no neighbor <neighborid> capability route-refresh
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*ipv6-addr*>|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode Router Configuration

Default Enabled

Usage Use this command to advertise to peer about route refresh capability support. If route refresh capability is supported, then router can dynamically request that the peer readvertises its Adj-RIB-Out.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 capability
route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 capability
route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.1.1 remote-as 10
awplus(config-router)# neighbor 10.10.1.1 peer-group group1
awplus(config-router)# neighbor group1 capability route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 capability
route-refresh
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 capability
route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 capability
route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 capability route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 capability
route-refresh
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor collide-established

Overview Use this command to specify including a BGP or BGP4+ neighbor, already in an 'established' state, for conflict resolution when a TCP connection collision is detected.

Use the **no** variant of this command to remove a BGP or BGP4+ neighbor, already in an 'established' state, for conflict resolution when a TCP connection collision is detected.

Syntax

```
neighbor <neighborid> collide-established
no neighbor <neighborid> collide-established
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode Router Configuration

Usage notes This command must be used only when specially required. It is not required in most network deployments.

The associated functionality of including an 'established' neighbor into TCP connection collision conflict resolution is automatically enabled when neighbor is configured for BGP graceful-restart.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1
collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 collide-established
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 collide-established
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor default-originate

Overview Use this command to allow a BGP or BGP4+ local router to send the default route to a neighbor.

Use the **no** variant of this command to send no route as a default route.

Syntax

```
neighbor {<neighborid>} default-originate [route-map
<routemap-name>]
```

```
no neighbor {<neighborid>} default-originate [route-map
<routemap-name>]
```

Parameter	Description	
<neighborid>	{*<ip-address>* | *<ipv6-addr>* | *<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
route-map	If a route-map is specified, then the route table must contain at least one route that matches the permit criteria of the route map before the default route will be advertised to the specified neighbor.	
<routemap-name>	Enter the route-map name.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 default-originate
route-map myroute
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 default-originate
route-map myroute
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.1
default-originate route-map myroute
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.1
default-originate route-map myroute
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 default-originate
route-map myroute
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 default-originate
route-map myroute
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
default-originate route-map myroute
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
default-originate route-map myroute
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 default-originate
route-map myroute
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 default-originate
route-map myroute
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor description

Overview Use this command to associate a description with a BGP or a BGP4+ neighbor. We recommend adding descriptions to defined neighbors, so any network administrators or network engineers can see a description of connected BGP or BGP4+ peers on the device.

Use the **no** variant of this command to remove the description from a BGP or a BGP4+ neighbor.

Syntax

```
neighbor <neighborid> description <description>
no neighbor <neighborid> description [<description>]
```

Parameter	Description	
<neighborid>	{*<ip-address>* | *<ipv6-addr>* | *<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<description>	Enter up to 80 characters of text describing the neighbor.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 description Backup
router for sales
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 description
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 description Backup
router for sales
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 description Backup
router for sales.
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 description
Backup router for sales
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
description
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 description Backup
router for sales
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 description Backup
router for sales
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor disallow-infinite-holdtime

Overview Use this command to disallow the configuration of infinite holdtime for BGP and BGP4+.

Use the **no** variant of this command to allow the configuration of infinite holdtime for BGP or BGP4+.

Syntax [BGP]

```
neighbor {<ip-address>} disallow-infinite-holdtime
no neighbor {<ip-address>} disallow-infinite-holdtime
```

Syntax [BGP4+]

```
neighbor {<ipv6-addr>} disallow-infinite-holdtime
no neighbor {<ipv6-addr>} disallow-infinite-holdtime
```

Parameter	Description
<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.

Mode Router Configuration

Usage This command enables the local BGP or BGP4+ speaker to reject holdtime "0" seconds from the peer during exchange of open messages or the user during configuration.

The **no** variant of this command allows the BGP speaker to accept "0" holdtime from the peer or during configuration.

Examples [BGP] To enable the **disallow-infinite-holdtime** feature on the BGP speaker with the IP address of `10.10.10.1`, enter the command:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1
disallow-infinite-holdtime
```

To disable the **disallow-infinite-holdtime** feature on the BGP speaker with the IP address of `10.10.10.10`, enter the command:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1
disallow-infinite-holdtime
```

Examples [BGP4+]

To enable the **disallow-infinite-holdtime** feature on the BGP4+ speaker with the IPv6 address of `2001:0db8:010d::1`, enter the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor
disallow-infinite-holdtime2001:0db8:010d::1
```

To disable the **disallow-infinite-holdtime** feature on the BGP4+ speaker with the IPv6 address of `2001:0db8:010d::1`, enter the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor
disallow-infinite-holdtime2001:0db8:010d::1
```

Related commands

neighbor timers

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor distribute-list

Overview This command filters route updates from a particular BGP or BGP4+ neighbor using an access control list.

You can add one incoming and one outgoing distribute-list for each BGP or BGP4+ neighbor.

The **no** variant of this command removes a previously configured BGP or BGP4+ distribute-list.

Syntax

```
neighbor <neighborid> distribute-list <access-list> {in|out}
no neighbor <neighborid> distribute-list <access-list> {in|out}
```

Parameter	Description	
<neighborid>	Specify an identification method for the BGP or BGP4+ peer. Use one of the following formats:	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) and neighbor route-map commands. When this parameter is used with this command, the command applies on all peers in the specified group.
<access-list>	The specific software access-list used to filter routes. Specify one of the following types of access-lists:	
	<name>	The name of an IP software access-list.
	<1-199>	The ID number of an IP software access-list.
	<1300-2699>	The ID number of an IP software access-list (expanded range).
in	Indicates that incoming advertised routes will be filtered.	
out	Indicates that outgoing advertised routes will be filtered.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Examples [BGP]

Example 1:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 distribute-list
mylist out
```

Example 2:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 distribute-list
mylist out
```

Example 3:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.1 distribute-list
mylist out
```

Example 4:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.1
distribute-list mylist out
```

Example 5:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor 10.10.10.1 distribute-list
mylist out
```

Example 6:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 distribute-list
mylist out
```

Examples [BGP4+]

Example 1:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
distribute-list mylist out
```

Example 2:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
distribute-list mylist out
```

Example 3:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor 2001:0db8:010d::1
distribute-list mylist out
```

Example 4:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
distribute-list mylist out
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor dont-capability-negotiate

Overview Use this command to disable capability negotiation for BGP and BGP4+.

The capability negotiation is performed by default. This command is used to allow compatibility with older BGP versions that have no capability parameters used in open messages between peers.

Use the **no** variant of this command to enable capability negotiation.

Syntax

```
neighbor <neighborid> dont-capability-negotiate
no neighbor <neighborid> dont-capability-negotiate
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the IPv4 address of the BGP neighbor in dotted decimal, in the format A.B.C.D.
	<ipv6-addr>	Specify the IPv6 address of the BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) and neighbor route-map commands. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode Router Configuration

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.34
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.34
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.34 remote-as 100
awplus(config-router)# neighbor 10.10.10.34 peer-group group1
awplus(config-router)# neighbor group1
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1
dont-capability-negotiate
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1
dont-capability-negotiate
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor ebgp-multihop

Overview Use this command to accept and attempt BGP or BGP4+ connections to external peers on indirectly connected networks.

Effectively, this command sets the TTL value in the BGP or BGP4+ packets that the router sends to the neighbor, so that the packets may traverse the network route to the neighbor.

The device will not establish a connection to a multihop neighbor, if the only route to the multihop peer is a default route.

Use the **no** variant of this command to return to the default.

Syntax

```
neighbor <neighborid> ebgp-multihop [<count>]
no neighbor <neighborid> ebgp-multihop [<count>]
```

Parameter	Description	
<neighborid>	{*<ip-address>* | *ipv6-addr* | *<peer-group>*}	
	<ip-addr>	Specify the address of an IPv4 BGP neighbor, entered in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<count>	*<1-255>* The Maximum hop count, that is set in the TTL field of the BGP packets. If this optional parameter is not specified with the command, then the Maximum hop count is set to 255.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.34 remote-as 10
awplus(config-router)# neighbor 10.10.10.34 ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.34 ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.34 remote-as 10
awplus(config-router)# neighbor 10.10.10.34 peer-group group1
awplus(config-router)# neighbor group1 ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 ebgp-multihop 5
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# neighbor 2001:0db8:010d::1
ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 ebgp-multihop 5
```

Related commands

neighbor ebgp-multihop

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor enforce-multihop

Overview Use this command to enforce the requirement that BGP and BGP4+ neighbors form multihop connections.

Use the **no** variant of this command to turn off this feature.

Syntax

```
neighbor <neighborid> enforce-multihop
no neighbor <neighborid> enforce-multihop
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	The address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.34 remote-as 10
awplus(config-router)# neighbor 10.10.0.34 enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.34 enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.34 remote-as 10
awplus(config-router)# neighbor 10.10.10.34 peer-group group1
awplus(config-router)# neighbor group1 enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 enforce-multihop
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# neighbor 2001:0db8:010d::1
enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 enforce-multihop
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor filter-list

Overview This command creates a BGP or BGP4+ filter using an AS (Autonomous System) path list. This command specifies an AS path list, which it then applies to filter updates to and from a BGP or a BGP4+ neighbor

The **no** variant of this command removes the previously specified BGP or BGP4+ filter using access control lists.

Syntax

```
neighbor <neighborid> filter-list <listname> {in|out}
no neighbor <neighborid> filter-list <listname> {in|out}
```

Parameter	Description	
<neighborid>	Specify the identification method for the BGP or BGP4+ peer. Use one of the following formats:	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<listname>	Specify the name of an AS (Autonomous System) path list.	
`in`	Indicates that incoming advertised routes will be filtered.	
`out`	Indicates that outgoing advertised routes will be filtered.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage This command specifies a filter for updates based on a BGP AS (Autonomous System) path list.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.34 filter-list list1
out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.34 filter-list list1
out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.0.34 filter-list list1
out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.0.34 filter-list
list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.34 remote-as 10
awplus(config-router)# neighbor 10.10.10.34 peer-group group1
awplus(config-router)# neighbor group1 filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 filter-list list1 out
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 filter-list list1
out
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor interface

Overview Use this command to configure the interface name of a BGP4+ speaking neighbor.

Use the **no** variant of this command to disable this function.

Syntax [BGP4+]

```
neighbor {<ipv6-addr>|<ipaddress>} interface <interface>
no neighbor {<ipv6-addr>|<ipaddress>} interface <interface>
```

Parameter	Description
<ipaddress>	Specifies the IPv4 address of the BGP neighbor - entered in dotted decimal notation in the format A.B.C.D.
<ipv6-addr>	Specifies the IPv6 address of the BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
<interface>	Specifies the interface name of BGP neighbor, e.g. `vlan2`.

Mode [BGP4+] Router Configuration

Usage [BGP4+] This command is for use with BGP4+ peering. Use this command for BGP peering with IPv6 link local addresses.

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 interface vlan2
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 interface vlan2
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 interface
vlan2
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 interface
vlan2
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor local-as

Overview Use this command to configure a local AS number for the specified BGP or BGP4+ neighbor. This overrides the local AS number specified by the router bgp command.

Use the **no** variant of this command to remove the local AS number for the specified BGP or BGP4+ neighbor.

Syntax

```
neighbor <neighborid> local-as <as-number>
no neighbor <neighborid> local-as <as-number>
```

Parameter	Description	
<neighborid>	{*<ip-address>* | *<ipv6-addr>* | *<peer-group>*}	
	<ip-address>	The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	The address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) and neighbor route-map commands. When this parameter is used with this command, the command applies on all peers in the specified group.
<as-number>	*<1-4294967295>* Neighbor's Autonomous System (AS) number.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Usage [BGP4+] When BGP4+ is configured, this command prepends the ASN as defined by the router bgp command, and adds the ASN as defined by the neighbor local-as command in front of the actual ASN as defined by the router bgp command. This makes the peer believe it is peering with the ASN as defined by the neighbor local-as command.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.34 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.34 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.34 remote-as 10
awplus(config-router)# neighbor 10.10.10.34 peer-group group1
awplus(config-router)# neighbor group1 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 local-as 1
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 local-as 1
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

router bgp

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor maximum-prefix

Overview Use this command to control the number of prefixes that can be received from a BGP or a BGP4+ neighbor.

Use the **no** variant of this command to disable this function. Do not specify threshold to apply the default threshold of 75% for the maximum number of prefixes before this is applied.

Syntax

```
neighbor <neighborid> maximum-prefix <maximum>
no neighbor <neighborid> maximum-prefix [<maximum>]
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<maximum>	*<maxprefix>*[*<threshold>*] [warning-only]	
<maxprefix>	*<1-4294967295>* Specifies the maximum number of prefixes permitted.	
<threshold>	*<1-100>* Specifies the threshold value, 1 to 100 percent. 75% by default.	
warning-only	Only gives a warning message when the limit is exceeded.	

Default The default threshold value is 75%. If the threshold value is not specified this default is applied.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage The **neighbor maximum-prefix** command allows the configuration of a specified number of prefixes that a BGP or a BGP4+ router is allowed to receive from a neighbor. When the warning-only option is not used, if any extra prefixes are received, the router ends the peering. A terminated peer, stays down until the **clear ip bgp** command is used.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 maximum-prefix 1244
warning-only
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 maximum-prefix
1244 warning-only
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.72 remote-as 10
awplus(config-router)# neighbor 10.10.10.72 peer-group group1
awplus(config-router)# neighbor group1 maximum-prefix 1244
warning-only
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 maximum-prefix 1244
warning-only
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
maximum-prefix 1244 warning-only
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
maximum-prefix 1244 warning-only
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 maximum-prefix 1244
warning-only
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 maximum-prefix
1244 warning-only
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor next-hop-self

Overview Use this command to configure the BGP or BGP4+ router as the next hop for a BGP or BGP4+ speaking neighbor or peer group.

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

Syntax

```
neighbor <neighborid> next-hop-self
no neighbor <neighborid> next-hop-self
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage notes This command allows a BGP or BGP4+ router to change the next hop information that is sent to the iBGP peer. The next hop information is set to the IP address of the interface used to communicate with the neighbor.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router)# neighbor 10.10.0.72 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router)# no neighbor 10.10.0.72 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.72 remote-as 10
awplus(config-router)# neighbor 10.10.10.72 peer-group group1
awplus(config-router)# neighbor group1 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 next-hop-self
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 next-hop-self
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor override-capability

Overview Use this command to override a capability negotiation result for BGP and BGP4+.

Use the **no** variant of with this command to disable this function.

Syntax

```
neighbor <neighborid> override-capability
no neighbor <neighborid> override-capability
```

Parameter	Description	
<neighborid>	{*<ip-address>* | *<ipv6-addr>* | *<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode Router Configuration

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 override-capability
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72
override-capability
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.72 remote-as 10
awplus(config-router)# neighbor 10.10.10.72 peer-group group1
awplus(config-router)# neighbor group1 override-capability
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 override-capability
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor 2001:0db8:010d::1
override-capability
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor 2001:0db8:010d::1
override-capability
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 override-capability
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor group1 override-capability
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor passive

Overview Use this command to configure the local BGP or BGP4+ router to be passive with regard to the specified BGP or BGP4+ neighbor. This has the effect that the BGP or BGP4+ router will not attempt to initiate connections to this BGP or BGP4+ neighbor, but will accept incoming connection attempts from the BGP or BGP4+ neighbor.

Use the **no** variant of this command to disable this function.

Syntax

```
neighbor <neighborid> passive
no neighbor <neighborid> passive
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.72 remote-as 10
awplus(config-router)# neighbor 10.10.10.72 peer-group group1
awplus(config-router)# neighbor group1 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 passive
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 passive
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor password

Overview Use this command to enable MD5 authentication on a TCP connection between BGP and BGP4+ neighbors. No authentication is applied by default. To setup authentication for the session, you must first apply authentication on each connected peer for the session.

Use the **no** variant of this command to disable this function.

Syntax [BGP]

```
neighbor {<ip-address>|<peer-group-name>} password <password>
no neighbor {<ip-address>|<peer-group-name>} password
[<password>]
```

Syntax [BGP4+]

```
neighbor {<ipv6-addr>|<peer-group-name>} password <password>
no neighbor {<ipv6-addr>|<peer-group-name>} password
[<password>]
```

Parameter	Description
<ip-address>	Specifies the IP address of the BGP neighbor, in A.B.C.D format.
<ipv6-addr>	Specifies the IPv6 address of the BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
<peer-group-name>	Name of an existing peer-group. When this parameter is used with this command, the command applies on all peers in the specified group.
<password>	An alphanumeric string of characters to be used as password.

Default No authentication is applied by default.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Usage notes When using the *<peer-group-name>* parameter with this command (to apply this command to all peers in the group), see the related commands neighbor peer-group (add a neighbor) and neighbor route-map for information about how to create peer groups first.

Examples [BGP] This example specifies the encryption type and the password 'manager' for the neighbor `10.10.10.1`:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 password manager
```

This example removes the password set for the neighbor `10.10.10.1`:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 password
```

This example specifies the encryption type and the password 'manager' for the neighbor peer group named 'group1':

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 password manager
```

This example removes the password set for the neighbor peer group named `group1`:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 password
```

Examples [BGP4+]

This example specifies the encryption type and the password 'manager' for the neighbor `2001:0db8:010d::1`:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor password manager
2001:0db8:010d::1
```

This example removes the password set for the neighbor `2001:0db8:010d::1`:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor password 2001:0db8:010d::1
```

This example specifies the encryption type and the password 'manager' for the neighbor peer group named `group1`:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor  remote-as 102001:0db8:010d::1
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor peer-group group1
2001:0db8:010d::1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 password manager
```

This example removes the password set for the neighbor peer group named 'group1':

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 password
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor peer-group (add a neighbor)

Overview Use this command to add a BGP or a BGP4+ neighbor to an existing peer-group.

Use the **no** variant of this command to disable this function.

Syntax [BGP]

```
neighbor <ip-address> peer-group <peer-group>
no neighbor <ip-address> peer-group <peer-group>
```

Syntax [BGP4+]

```
neighbor <ipv6-addr> peer-group <peer-group>
no neighbor <ipv6-addr> peer-group <peer-group>
```

Parameter	Description
<ip-address>	Specify the IPv4 address of the BGP neighbor, entered in the format A.B.C.D.
<ipv6-addr>	Specify the IPv6 address of the BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
<peer-group>	Enter the name of the peer-group. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage Use this command to add neighbors with the same update policies to a peer group. This facilitates the updates of various policies, such as, distribute and filter lists. The peer-group is then configured easily with many of the neighbor commands. Any changes made to the peer group affect all members.

To create a peer-group use the neighbor port command and then use this command to add neighbors to the group.

Examples [BGP] This example shows a new peer-group `group1` and the addition of a neighbor `10.10.0.63` to the group.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.63 peer-group group1
```

This example shows a new peer-group `group1` and the removal of a neighbor `10.10.0.63` to the group.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# no neighbor 10.10.0.63 peer-group group1
```

Examples [BGP4+]

This example shows a new peer-group `group1` and the addition of a neighbor `2001:0db8:010d::1` to the group.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor  peer-group
group12001:0db8:010d::1
```

This example shows a new peer-group `group1` and the removal of a neighbor `2001:0db8:010d::1` to the group.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor  peer-group
group12001:0db8:010d::1
```

Related commands

neighbor peer-group (create a peer-group)

neighbor port

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor peer-group (create a peer-group)

Overview Use this command to create a peer-group for BGP and BGP4+.

Use the **no** variant of this command to disable this function.

Syntax

```
neighbor <peer-group> peer-group
no neighbor <peer-group> peer-group
```

Parameter	Description
<peer-group>	Enter the name of the peer-group.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Usage notes Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as, distribute and filter lists.

The peer-group is then configured easily with many of the neighbor commands. Any changes made to the peer group affect all members.

Use this command to create a peer-group, then use the neighbor peer-group (add a neighbor) command to add neighbors to the group.

Examples

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 peer-group
```

Related commands neighbor peer-group (add a neighbor)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor port

Overview Use this command to specify the TCP port to which packets are sent to on a BGP or a BGP4+ neighbor. TCP port 179 is the default port used to connect BGP and BGP4+ peers. You can specify a different destination port for the TCP session with this command.

Use the **no** variant of this command to reset the port number back to the default value (TCP port 179).

Syntax [BGP]

```
neighbor <neighborid> port <portnum>
no neighbor <neighborid> port [<portnum>]
```

Parameter	Description	
<neighborid>	{*<ip-address>* | *ipv6-addr>* | *<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<portnum>	*<0-65535>* Specifies the TCP port number.	

Default TCP port 179 is the default port used to connect BGP and BGP4+ peers.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor 10.10.10.10 port 643
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor 10.10.10.10 port 643
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 port 643
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor group1 port 643
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor  port 6432001:0db8:010d::1
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor  port 6432001:0db8:010d::1
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(awplus-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 port 643
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor group1 port 643
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor prefix-list

Overview Use this command to distribute BGP and BGP4+ neighbor information as specified in a prefix list.

Use the **no** variant of this command to remove an entry.

Syntax

```
neighbor <neighborid> prefix-list <listname> {in|out}
no neighbor <neighborid> prefix-list <listname> {in|out}
```

Parameter	Description	
<neighborid>	*<ip-address>*|*<ipv6-addr>*|*<peer-group>*	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<listname>	The name of an IP prefix list.	
in	Specifies that the IP prefix list applies to incoming advertisements.	
out	Specifies that the IP prefix list applies to outgoing advertisements.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage notes Use this command to specify a prefix list for filtering BGP or BGP4+ advertisements. Filtering by prefix list matches the prefixes of routes with those listed in the prefix list. If there is a match, the route is used. An empty prefix list permits all prefixes. If a given prefix does not match any entries of a prefix list, the route is denied access.

The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router does not need to go through the rest of the prefix list. For efficiency the most common matches or denies are listed at the top.

The **neighbor distribute-list** command is an alternative to the **neighbor prefix-list** command and only one of them can be used for filtering to the same neighbor in any direction.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# ip prefix-list list1 deny 30.0.0.0/24
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 prefix-list list1 in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 prefix-list list1
in
awplus# configure terminal
awplus(config)# ip prefix-list list1 deny 30.0.0.0/24
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.1 prefix-list list1
in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.1 prefix-list
list1 in
awplus# configure terminal
awplus(config)# ip prefix-list list1 deny 30.0.0.0/24
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 prefix-list list1 in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 prefix-list list1 in
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# ipv6 prefix-list list1 deny
2001:0db8:010d::1/128
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:: prefix-list
list1 in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:: prefix-list
list1 in
awplus# configure terminal
awplus(config)# ip prefix-list list1 deny 2001:0db8:010d::1/128
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 prefix-list list1 in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 prefix-list list1
in
```

Related commands

ip prefix-list

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor remote-as

Overview Use this command to configure an internal or external BGP or BGP4+ (iBGP or eBGP) peering relationship with another router.

Use the **no** variant of this command to remove a previously configured BGP or BGP4+ peering relationship.

Syntax

```
neighbor <neighborid> remote-as <as-number>
no neighbor <neighborid> remote-as <as-number>
```

Parameter	Description	
<neighborid>	{*<ip-address>* | *ipv6-addr>* | *<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<as-number>	*<1-4294967295>* Neighbor's Autonomous System (AS) number.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Usage notes This command is used to configure iBGP and eBGP peering relationships with other BGP or BGP4+ neighbors. A peer-group support of this command is configured only after creating a specific peer-group. Use the **no** variant of this command to remove a previously configured BGP peering relationship.

Examples [BGP] To configure a BGP peering relationship from the neighbor with the IPv4 address 10.10.0.73 with another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.73 remote-as 10
```

To remove a configured BGP peering relationship from the neighbor with the IPv4 address 10.10.0.73 from another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.73 remote-as 10
```

To configure a BGP peering relationship from the neighbor with the peer group named group1 with another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 remote-as 10
```

To remove a configured BGP peering relationship from the neighbor with the peer group named group1 with another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 remote-as 10
```

Examples [BGP4+]

To configure a BGP4+ peering relationship with another router:

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 345
```

To remove a configured BGP4+ peering relationship from another router:

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# no neighbor 2001:0db8:010d::1 remote-as
345
```

To configure a BGP4+ peering relationship from the neighbor with the peer group named group1 with another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 remote-as 10
```

To remove a configured BGP4+ peering relationship from the neighbor with the peer group named group1 with another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 remote-as 10
```

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor remove-private-AS (BGP only)

Overview Use this command to remove the private Autonomous System (AS) number from external outbound updates. Use the **no** variant of this command to revert to the default (disabled).

Syntax

```
neighbor <neighborid> remove-private-AS
no neighbor <neighborid> remove-private-AS
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<tag>*}	
	<ip-address>	The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<tag>	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor remote-as command. When this parameter is used with a command, the command applies on all peers in the specified group.

Default This command is disabled by default.

Mode Router Configuration or IPv4 Address Family Configuration

Usage notes The private AS numbers range from <64512-65535>. Private AS numbers are not advertised to the Internet. This command is used with external BGP peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.

This command removes private AS numbers for BGP in Router Configuration mode. This command is not supported for BGP4+ in IPv6 Address Family Configuration mode. This command removes a private AS number and makes an update packet with a public AS number as the AS path attribute. So only public AS numbers are entered in Internet BGP routing tables, and private AS numbers are not entered in Internet BGP tables.

For the filtering to apply, both peering devices must be set to use either 2-byte or extended 4- byte ASN (with the same ASN type set on both peers). For example, if a device (which defaults to use a 4-byte ASN), is peered with a device that defaults to a 2-byte ASN, then the device using a 2-byte ASN device also needs to be configured with the command **bgp extended-asn-cap** for the filtering to apply.

Examples

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.63 remove-private-AS
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.63 remove-private-AS
```

Related commands

show ip bgp (BGP only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor restart-time

Overview Use this command to set a different restart-time other than the global restart-time configured using the **bgp graceful-restart** command for BGP and BGP4+.

Use the **no** variant of this command to restore the device to its default state (see the default value of the **bgp graceful-restart** command).

Syntax

```
neighbor <neighborid> restart-time <delay-value>
no neighbor <neighborid> restart-time <delay-value>
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<delay-value>	*<1-3600>*	Delay value in seconds.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Usage This command takes precedence over the restart-time value specified using the **bgp graceful-restart** command.

The restart-time value is the maximum time that a graceful-restart neighbor waits to come back up after a restart. The default is 120 seconds.

Make sure that the restart time specified using this command does not exceed the stalepath-time specified in the Router Configuration mode.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 restart-time 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 restart-time 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 restart-time 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 restart-time 45
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 restart-time
45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
restart-time 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 restart-time 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 restart-time 45
```

Related commands

bgp graceful-restart

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor route-map

Overview Use this command to apply a route map to incoming or outgoing routes for BGP or BGP4+.

Use the **no** variant of this command to remove a route map from a BGP or BGP4+ route.

Syntax

```
neighbor <neighborid> route-map <mapname> {in|out}
no neighbor <neighborid> route-map <mapname> {in|out}
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*ipv6-addr*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<mapname>	Specifies name of the route-map.	
in	Specifies that the access list applies to incoming advertisements.	
out	Specifies that the access list applies to outgoing advertisements.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage notes Use the **neighbor route-map** command to filter updates and modify attributes. A route map is applied to inbound or outbound updates. Only the routes that pass the route map are sent or accepted in updates.

Examples [BGP] The following example shows the configuration of the route-map name **rmap2** and then the use of this map name in the **neighbor route-map** command for the neighbor with the IPv4 address 10.10.10.1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 6
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 route-map rmap2 in
```

The following example shows the removal of the route-map name **rmap2** in the **neighbor route-map** command for the neighbor with the IPv4 address 10.10.10.1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 route-map rmap2
in
```

The following example shows the configuration of the route-map name **rmap2** and then the use of this map name in the **neighbor route-map** command for the neighbor with the IPv4 address 10.10.10.1 in the IPv4 Address Family Configuration mode.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 6
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.1 route-map rmap2
in
```

The following example shows the removal of the route-map name **rmap2** in the **neighbor route-map** command for the neighbor with the IPv4 address 10.10.10.1 in the IPv4 Address Family Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.1 route-map
rmap2 in
```

The following example shows the configuration of the route-map name **rmap2** and then the use of this map name in the **neighbor route-map** command for the neighbor with the peer group named group1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 6
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 route-map rmap2 in
```

The following example shows the removal the route-map name **rmap2** in the **neighbor route-map** command for the neighbor with the peer group named group1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 route-map rmap2 in
```

Examples [BGP4+]

The following example shows the configuration of the route-map name **rmap2** and then the use of this map name in the **neighbor route-map** command for the neighbor with the IPv6 address 2001:0db8:010d::1 in the IPv6 Address Family Configuration mode.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 6
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1 route-map
rmap2 in
```

The following example shows the removal of the route-map name **rmap2** in the **neighbor route-map** command for the neighbor with the IPv6 address 2001:0db8:010d::1 in the IPv6 Address Family Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
route-map rmap2 in
```

The following example shows the configuration of the route-map name **rmap2** and then the use of this map name in the **neighbor route-map** command for the neighbor with the peer group named group1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 6
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 route-map rmap2 in
```

The following example shows the removal the route-map name **rmap2** in the **neighbor route-map** command for the neighbor with the peer group named group1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 route-map rmap2 in
```

Related commands

address-family

neighbor peer-group (add a neighbor)

route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor route-reflector-client (BGP only)

Overview Use this command to configure the router as a BGP route reflector and configure the specified neighbor as its client.

Use the **no** variant of this command to indicate that the neighbor is not a client.

Syntax

```
neighbor <neighborid> route-reflector-client
no neighbor <neighborid> route-reflector-client
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<peer-group>*}	
	<ip-address>	The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode Router Configuration or IPv4 Address Family Configuration

Usage notes Route reflectors are a solution for the explosion of iBGP peering within an autonomous system. By route reflection the number of iBGP peers within an AS is reduced. Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and specify neighbors as its client.

An AS can have more than one route reflector. One route reflector treats the other route reflector as another iBGP speaker.

In the following configuration, Router1 is the route reflector for clients `3.3.3.3` and `2.2.2.2`; it also has a non-client peer `6.6.6.6`:

```
Router1#
router bgp 200
neighbor 3.3.3.3 remote-as 200
neighbor 3.3.3.3 route-reflector-client
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 route-reflector-client
neighbor 6.6.6.6 remote-as 200
```

Examples

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72
route-reflector-client
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72
route-reflector-client
```

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor route-server-client (BGP only)

Overview Use this command to specify the peer as route server client.

Use the **no** variant of this command to disable this function.

Syntax

```
neighbor <neighborid> route-server-client
no neighbor <neighborid> route-server-client
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<peer-group>*}	
	<ip-address>	The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode Router Configuration

Examples

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 route-server-client
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72
route-server-client
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor send-community

Overview Use this command to specify that a community attribute should be sent to a BGP or BGP4+ neighbor.

Use the **no** variant of this command to remove the entry for the community attribute.

Syntax

```
neighbor <neighborid> send-community {both|extended|standard}
no neighbor <neighborid> send-community
{both|extended|standard}
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
`both`	Sends Standard and Extended Community attributes. Specifying this parameter with the **no** variant of this command results in no `standard` or `extended` community attributes being sent.	
`extended`	Sends Extended Community attributes. Specifying this parameter with the **no** variant of this command results in no `extended` community attributes being sent.	
`standard`	Sends Standard Community attributes. Specifying this parameter with the **no** variant of this command results in no `standard` community attributes being sent.	

Default Both **standard** and **extended** community attributes are sent to a neighbor.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration and IPv6 Address Family Configuration

Usage notes This command is used to specify a community attribute to be sent to a neighbor. The community attribute groups destinations in a certain community and applies routing decisions according to those communities. On receiving community attributes the router reannounces them to the neighbor. Only when the **no**

parameter is used with this command the community attributes are not reannounced to the neighbor.

By default, both **standard** and **extended** community attributes are sent to a neighbor.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 send-community
extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 send-community
extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.0.72 send-community
extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.0.72 send-community
extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 send-community extended
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
send-community extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
send-community extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
send-community extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
send-community extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 send-community extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 send-community
extended
```

Related commands

bgp config-type

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor shutdown

Overview Use this command to disable a peering relationship with a BGP or BGP4+ neighbor.

Use the **no** variant of this command to re-enable the BGP or BGP4+ neighbor.

Syntax

```
neighbor <neighborid> shutdown
no neighbor <neighborid> shutdown
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Usage notes This command shuts down any active session for the specified BGP or BGP4+ neighbor and clears all related routing data.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 shutdown
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 shutdown
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor soft-reconfiguration inbound

Overview Use this command to configure the device to start storing all updates from the BGP or BGP4+ neighbor, without any consideration of any inward route filtering policy that might be applied to the connection with this BGP or BGP4+ neighbor. This is so that the full set of the neighbor's updates are available locally to be used in a soft-reconfiguration event.

You may need to apply this older method of clearing routes if the peer does not support route refresh.

Use the **no** variant of this command to disable this function for a BGP or BGP4+ neighbor.

Syntax

```
neighbor <neighborid> soft-reconfiguration inbound
no neighbor <neighborid> soft-reconfiguration inbound
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage Use this command to store updates for inbound soft reconfiguration. Soft-reconfiguration may be used in lieu of BGP route refresh capability. Using this command enables local storage of all the received routes and their attributes. This requires additional memory. When a soft reset (inbound) is done on this neighbor, the locally stored routes are re- processed according to the inbound policy. The BGP neighbor connection is not affected.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor 10.10.10.10
soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor 10.10.10.10
soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# address-family ipv4
awplus(config-router-
af)# neighbor 10.10.10.10 soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# address-family ipv4
awplus(config-router-
af)# no neighbor 10.10.10.10 soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 soft-reconfiguration
inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor group1 soft-reconfiguration
inbound
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 soft-reconfiguration
inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# address-family ipv6
awplus(config-router-
af)# no neighbor group1 soft-reconfiguration inbound
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor timers

Overview Use this command to set the keepalive, holdtime, and connect timers for a specific BGP or BGP4+ neighbor.

Use the **no** variant of this command to clear the timers for a specific BGP or BGP4+ neighbor.

Syntax

```
neighbor <neighborid> timers {<keepalive> <holdtime>|connect <connect>}
no neighbor <neighborid> timers [connect]
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<keepalive>	*<0-65535>* Frequency (in seconds) at which a router sends keepalive messages to its neighbor.	
<holdtime>	*<0-65535>* Interval (in seconds) after which, on not receiving a keepalive message, the router declares a neighbor dead.	
<connect>	connect *<1-65535>* Specifies the connect timer in seconds. The default connect timer value is 120 seconds as per RFC 4271. Modify this value as needed for interoperability.	

Default The keepalive timer default is 60 seconds, the holdtime timer default is 90 seconds, and the connect timer default is 120 seconds as per RFC 4271. Holdtime is keepalive * 3.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Usage Keepalive messages are sent by a router to inform another router that the BGP connection between the two is still active. The keepalive interval is the period of time between each keepalive message sent by the router. The holdtime interval is the time the router waits to receive a keepalive message and if it does not receive

a message for this period it declares the neighbor dead. The holdtime value must be 3 times the value of the keepalive value.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 timers 60 120
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 timers
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 timers 60 120
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 timers
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 timers 60 120
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 timers
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 timers 60 120
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 timers
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

show ip bgp neighbors hold-time (BGP only)

show ip bgp neighbors keepalive-interval (BGP only)

timers (BGP)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor transparent-as

Overview Use this command to specify not to append your AS path number even if the BGP or BGP4+ peer is an eBGP peer.

Note this command has the same effect as invoking neighbor attribute-unchanged and specifying the optional **as-path** parameter.

Syntax

```
neighbor <neighborid> transparent-as
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode Router Configuration

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 transparent-as
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 transparent-as
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
transparent-as
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 transparent-as
```

Related commands

neighbor attribute-unchanged

neighbor peer-group (add a neighbor)

neighbor route-map

neighbor transparent-nexthop

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor transparent-nexthop

Overview Use this command to keep the next hop value of the route even if the BGP or BGP4+ peer is an eBGP peer.

Note this command has the same effect as invoking neighbor attribute-unchanged and specifying the optional **next-hop** parameter.

Syntax

```
neighbor <neighborid> transparent-nexthop
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<ipv6-addr>*|*<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.

Mode Router Configuration

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 transparent-nexthop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 transparent-nexthop
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
transparent-nexthop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 transparent-nexthop
```

Related commands

neighbor attribute-unchanged

neighbor peer-group (add a neighbor)

neighbor route-map

neighbor transparent-as

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor unsuppress-map

Overview Use this command to selectively leak more specific routes to a particular BGP or BGP4+ neighbor.

Use the **no** variant of this command to remove selectively leaked specific routes to a particular BGP or BGP4+ neighbor.

Syntax

```
neighbor <neighborid> unsuppress-map <route-map-name>
no neighbor <neighborid> unsuppress-map <route-map-name>
```

Parameter	Description	
<neighborid>	{*<ip-address>* | *<ipv6-addr>* | *<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<route-map-name>	The name of the route-map used to select routes to be unsuppressed.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage When the aggregate-address command is used with the **summary-only** option, the more-specific routes of the aggregate are suppressed to all neighbors. Use this command instead to selectively leak more-specific routes to a particular neighbor.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.73 unsuppress-map mymap
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4 unicast
awplus(config-router-af)# neighbor 10.10.0.70 unsuppress-map
mymap
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.73 unsuppress-map
mymap
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4 unicast
awplus(config-router-af)# no neighbor 10.10.0.70 unsuppress-map
mymap
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 unsuppress-map mymap
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 unsuppress-map mymap
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6 unicast
awplus(config-router-af)# neighbor 2001:0db8:010d::1
unsuppress-map mymap
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6 unicast
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
unsuppress-map mymap
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 unsuppress-map mymap
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 unsuppress-map
mymap
```

Related commands

aggregate-address

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor update-source

Overview Use this command to specify the source IPv4 or IPv6 address of BGP or BGP4+ packets, which are sent to the neighbor for routing updates, as the IPv4 or IPv6 address configured on the specified interface. The specified interface is usually the local loopback (lo) interface to allow internal BGP or BGP4+ connections to stay up regardless of which interface is used to reach a neighbor.

Use the **no** variant of this command to remove the IPv4 or IPv6 address from the interface as the source IPv4 or IPv6 address of BGP or BGP4+ packets sent to the neighbor, and restores the interface assignment to the closest interface, which is also called the best local address.

Syntax

```
neighbor <neighborid> update-source <interface>
no neighbor <neighborid> update-source
```

Parameter	Description	
<neighborid>	{*<ip-address>* | *<ipv6-addr>* | *<peer-group>*}	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<interface>	Specifies the local loopback interface (lo).	

Default Use of this command sets a default value of 2 for the maximum hop count.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration

Usage Use this command in conjunction with any specified interface on the router. The local loopback interface is the interface that is most commonly used with this command. The use of local loopback interface eliminates a dependency and BGP or BGP4+ does not have to rely on the availability of a particular interface for making BGP or BGP4+ peer relationships.

Examples [BGP] To source BGP connections for neighbor 10.10.0.72 with the IP address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.0.73/24
awplus(config-if)# exit
awplus(config)# router bgp 100
awplus(config-router)# network 10.10.0.0
awplus(config-router)# neighbor 10.10.0.72 remote-as 110
awplus(config-router)# neighbor 10.10.0.72 update-source lo
```

To remove BGP connections for neighbor 10.10.0.72 with the IP address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# router bgp 100
awplus(config-router)# no neighbor 10.10.0.72 update-source
```

To source BGP connections for neighbor group1 with the IP address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.0.73/24
awplus(config-if)# exit
awplus(config)# router bgp 100
awplus(config-router)# network 10.10.0.0
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.72 remote-as 100
awplus(config-router)# neighbor 10.10.0.72 peer-group group1
awplus(config-router)# neighbor group1 update-source lo
```

To remove BGP connections for neighbor group1 with the IP address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# router bgp 100
awplus(config-router)# neighbor group1 update-source lo
```

Examples [BGP4+]

To source BGP connections for neighbor 2001:0db8:010d::1 with the IPv6 address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# interface lo
awplus(config-if)# ipv6 address 2001:0db8:010d::1/128
awplus(config-if)# exit
awplus(config)# router bgp 100
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 110
awplus(config-router)# neighbor 2001:0db8:010d::1
update-source lo
```

To remove BGP connections for neighbor 2001:0db8:010d::1 with the IPv6 address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# router bgp 100
awplus(config-router)# no neighbor 2001:0db8:010d::1
update-source
```

To source BGP connections for neighbor group1 with the IPv6 address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# interface lo
awplus(config-if)# ipv6 address 2001:0db8:010d::1/128
awplus(config-if)# exit
awplus(config)# router bgp 100
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 100
awplus(config-router)# address-family ipv6
awplus(config-router-
af)# neighbor 2001:0db8:010d::1 peer-group group1
awplus(config-router-
af)# exit
awplus(config-router)# neighbor group1 update-source lo
```

To remove BGP connections for neighbor group1 with the IPv6 address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# router bgp 100
awplus(config-router)# neighbor group1 update-source lo
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor version (BGP only)

Overview Use this command to configure the device to accept only a particular BGP version.

Use the **no** variant of this command to use the default BGP version (version 4).

Syntax

```
neighbor <neighborid> version <version>
no neighbor <neighborid> version
```

Parameter	Description	
<neighborid>	{*<ip-address>*|*<peer-group>*}	
	<ip-address>	The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<peer-group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<version>	{4} Specifies the BGP version number.	

Mode Router Configuration or IPv4 Address Family Configuration

Usage notes By default, the system uses BGP version 4 and on request dynamically negotiates down to version 2. Using this command disables the router's version-negotiation capability and forces the router to use only a specified version with the neighbor.

Examples

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 version 4
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 version 4
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 version
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 version
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

neighbor weight

Overview Use this command to set default weights for routes from this BGP or BGP4+ neighbor.

Use the **no** variant of this command to remove a weight assignment.

Syntax

```
neighbor <neighborid> weight <weight>
no neighbor <neighborid> weight [<weight>]
```

Parameter	Description	
<neighborid>	*{<ip-address>|<ipv6-addr>|<peer-group>}*	
	<ip-address>	Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
	<ipv6-addr>	Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.
	<peer- group>	Enter the name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group (add a neighbor) command, and neighbor route-map command. When this parameter is used with this command, the command applies on all peers in the specified group.
<weight>	*<0-65535>* Specifies the weight this command assigns to the route.	

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage notes Use this command to specify a weight value to all routes learned from a BGP or BGP4+ neighbor. The route with the highest weight gets preference when there are other routes on the network.

Unlike the local-preference attribute, the weight attribute is relevant only to the local router.

The weights assigned using the **set weight** command overrides the weights assigned using this command.

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 weight 60
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 weight
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.1 weight 60
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.1 weight
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 weight 60
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 weight
```

Examples [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1 weight 60
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1 weight
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 weight 60
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 weight
```

Related commands

neighbor peer-group (add a neighbor)

neighbor route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

network (BGP and BGP4+)

Overview Use this command to specify particular routes to be advertised into the BGP or BGP4+ routing process. A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

Note that you can specify a prefix length for the prefix being added, and you can also specify a classful network without a prefix length and an appropriate prefix length is added. Note that specifying a non-classful prefix without a prefix length results in a /32 prefix length on an IPv4 route.

Use the **no** variant of this command to remove a network route entry.

Syntax [BGP]

```
network {<ip-prefix/length>|<ip-network-addr>} [mask
<network-mask>] [route-map <route-map-name>] [backdoor]
```

```
no network {<ip-prefix/length>|<ip-network-addr>} [mask
<network-mask>] [route-map <route-map-name>] [backdoor]
```

Syntax [BGP4+]

```
network {<ipv6-prefix/length>|<ipv6-network-addr>} [route-map
<route-map-name>]
```

```
no network {<ipv6-prefix/length>|<ipv6-network-addr>}
[route-map <route-map-name>]
```

Parameter	Description
<ip-prefix/length>	IP network prefix and prefix length entered in dotted decimal format for the IP network prefix, then slash notation for the prefix length in the format A.B.C.D/M, e.g. 192.168.1.224/27
<ip-network-addr>	IP network prefix entered in dotted decimal format A.B.C.D, e.g. 192.168.1.224
<network-mask>	Specify a network mask in the format A.B.C.D, e.g. 255.255.255.224.
<ipv6-prefix/length>	IPv6 network prefix and prefix length entered in dotted decimal format for the IPv6 network prefix, then slash notation for the IPv6 prefix length in the format X:X::X:X/M, e.g. 2001:db8::/64
<ipv6-network-addr>	IP network prefix entered in dotted decimal format A.B.C.D, e.g. 192.168.1.224
<route-map-name>	Specify the name of the route map.
backdoor	Specify a BGP backdoor route that is not advertised.

Mode [BGP] Router Configuration and IPv4 Address Family `ipv4 unicast` mode

Mode [BGP4+] IPv6 Address Family Configuration

Usage notes

It does not matter how the route is arranged in the IP or IPv6 routing table. The route can arrive in the IP routing table by a static route, or the route can be learned from OSPF or OSPFv3 or RIP or RIPng routing.

If you configure a route-map, then that route-map will be used in filtering the network, or the route-map will be used to modify the attributes that are advertised with the route.

Example [BGP]

The following example illustrates a Class-A address configured as a network route. The natural Class-A network prefix mask length of 8 will be internally derived, that is, 2.0.0.0/8.

```
awplus(config)# router bgp 100
awplus(config-router)# network 2.0.0.0
```

Output [BGP]

Figure 30-1: Example output from the **show running-config** command after entering **network 2.0.0.0**

```
awplus#show running-config

router bgp 100
 network 2.0.0.0/8
```

Example [BGP]

The following example illustrates a network address which does not fall into its natural class boundary, and hence, is perceived as a host route, that is, 192.0.2.224/27.

```
awplus(config)# router bgp 100
awplus(config-router)# network 192.0.2.224 mask 255.255.255.224
```

Output [BGP]

Figure 30-2: Example output from the **show running-config** command after entering **network 192.0.2.224 mask 255.255.255.224**

```
awplus#show running-config

router bgp 100
 network 192.0.2.224/27
```

Example [BGP]

The following example is the same as the previous example for host route 192.0.2.224/27, but is entered in prefix/length format using slash notation (instead of prefix plus mask in dotted decimal format using the **mask** keyword before the network mask in dotted decimal format):

```
awplus(config)# router bgp 100
awplus(config-router)# network 192.0.2.224/27
```

Example [BGP4+]

The following example is the same as the previous example for host route 2001:db8::/32:

```
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# network 2001:db8::/32
```

Output [BGP4+]

Figure 30-3: Example output from the **show running-config** command after entering **network 2001:db8::/32**

```
awplus#show running-config

router bgp 100
 network 2001:db8::/32
```

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

network synchronization

Overview Use this command to ensure the exact same static network prefix, specified through any of the **network** commands, is local or has IGP reachability before introduction to BGP or BGP4+.

Use the **no** variant of this command to disable this function.

Syntax

```
network synchronization
no network synchronization
```

Default Network synchronization is disabled by default.

Mode [BGP] Router Configuration and IPv4 Address Family [ipv4 unicast] Configuration

Mode [BGP4+] IPv6 Address Family [ipv6 unicast] Configuration

Examples [BGP] The following example enables IGP synchronization of BGP static network routes in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# network synchronization
```

The following example enables IGP synchronization of BGP static network routes in the IPv4-Unicast address family.

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# address-family ipv4 unicast
awplus(config-router-af)# network synchronization
```

Example [BGP4+] The following example enables IGP synchronization of BGP4+ static network routes in the IPv6-Unicast address family.

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# address-family ipv6 unicast
awplus(config-router-af)# network synchronization
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

redistribute (into BGP or BGP4+)

Overview Use this command to inject routes from one routing process into a BGP or BGP4+ routing table.

Use the **no** variant of this command to disable this function.

Syntax

```
redistribute {ospf|rip|connected|static} [route-map
<route-map-entry-pointer>]
```

```
no redistribute {ospf|rip|connected|static} [route-map
<route-map-entry-pointer>]
```

Parameter	Description
`connected`	Specifies the redistribution of connected routes for both BGP and BGP4+.
`ospf`	Specifies the redistribution of OSPF information for BGP or OSPFv3 information for BGP4+.
`rip`	Specifies the redistribution of RIP information for BGP or RIPng information for BGP4+.
`static`	Specifies the redistribution of Static routes for both BGP and BGP4+.
`route-map`	Route map reference for both BGP and BGP4+.
`<route-map-entry-pointer>`	Pointer to route-map entries.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] Router Configuration or IPv6 Address Family Configuration

Usage notes Redistribution is used by routing protocols to advertise routes that are learned by some other means, such as by another routing protocol or by static routes. Since all internal routes are dumped into BGP, careful filtering is applied to make sure that only routes to be advertised reach the internet, not everything. This command allows redistribution by injecting prefixes from one routing protocol into another routing protocol.

Examples [BGP/ BGP+] The following example shows the configuration of a route-map named `rmap1`, which is then applied using the **redistribute route-map** command.

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 1
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 12
awplus(config-router)# redistribute ospf route-map rmap1
```

The following example shows the configuration of a route-map named `rmap2`, which is then applied using the **redistribute route-map** command.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 3
awplus(config-route-map)# match interface vlan1
awplus(config-route-map)# set metric-type 1
awplus(config-route-map)# exit
awplus(config)# router ospf 100
awplus(config-router)# redistribute bgp route-map rmap2
```

Note that configuring a route-map and applying it with the redistribute route-map command allows you to filter which router are distributed from another routing protocol (such as OSPF with BGP). A route-map can also set the metric, tag, and metric-type of the redistributed routes.

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

restart bgp graceful (BGP only)

Overview Use this command to force the device to perform a graceful BGP restart.

Syntax

```
restart bgp graceful
```

Mode Privileged Exec

Usage Before using this command, BGP graceful-restart capabilities must be enabled within the router BGP (bgp graceful-restart command), and each neighbor configured on the device should be set to advertise its graceful-restart capability (bgp graceful-restart graceful-reset command). The neighbor devices also need to have BGP graceful-restart capabilities enabled (bgp graceful-restart command).

This command stops the whole BGP process and makes the device retain the BGP routes and mark them as stale. Receiving BGP speakers, retain and mark as stale all BGP routes received from the restarting speaker for all the address families received in the Graceful Restart Capability exchange.

When a **restart bgp graceful** command is issued, the BGP configuration is reloaded from the last saved configuration. Ensure you first issue a **copy running-config startup-config**.

Example

```
awplus# restart bgp graceful
```

Related commands

bgp graceful-restart

bgp graceful-restart graceful-reset

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

router bgp

Overview Use this command to configure a BGP routing process, specifying the 32-bit Autonomous System (AS) number.

Use the **no** variant of this command to disable a BGP routing process, specifying the 32-bit AS number.

Syntax

```
router bgp <asn>
no router bgp <asn>
```

Parameter	Description
<asn>	*<1-4294967295>* Specifies the 32-bit Autonomous System (AS) number.

Mode Global Configuration

Usage The **router bgp** command enables a BGP routing process:

```
router bgp 1
    neighbor 10.0.0.1 remote-as 1
    neighbor 10.0.0.2 remote-as 1
     !
  router bgp 2
    neighbor 10.0.0.3 remote-as 2
    neighbor 10.0.0.4 remote-as 2
```

Examples

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)#
awplus# configure terminal
awplus(config)# no router bgp 12
awplus(config)#
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

route-map

Overview Use this command to configure a route map entry, and to specify whether the device will process or discard matching routes and BGP update messages.

The device uses a name to identify the route map, and a sequence number to identify each entry in the route map.

The **route-map** command puts you into route-map configuration mode. In this mode, you can use the following:

- one or more of the **match** commands to create match clauses. These specify what routes or update messages match the entry.
- one or more of the **set** commands to create set clauses. These change the attributes of matching routes or update messages.

Use the **no** variant of this command to delete a route map or to delete an entry from a route map.

Syntax

```
route-map <mapname> {deny|permit} <seq>
no route-map <mapname>
no route-map <mapname> {deny|permit} <seq>
```

Parameter	Description
<mapname>	A name to identify the route map.
`deny`	The route map causes a routing process to discard matching routes or BGP update messages.
`permit`	The route map causes a routing process to use matching routes or BGP update messages.
<seq>	<1-65535> The sequence number of the entry. You can use this parameter to control the order of entries in this route map.

Mode Global Configuration

Usage notes Route maps allow you to control and modify routing information by filtering routes and setting route attributes. You can apply route maps when the device:

- processes BGP update messages that it has received from a peer
- prepares BGP update messages to send to peers
- redistributes routes from one routing protocol into another
- redistributes static routes into routing protocols
- uses BGP route flap dampening

When a routing protocol passes a route or update message through a route map, it checks the entries in order of their sequence numbers, starting with the lowest numbered entry.

If it finds a match on a route map with an action of permit, then it applies any set clauses and accepts the route. Having found a match, the route is not compared against any further entries of the route map.

If it finds a match on a route map with an action of deny, it will discard the matching route.

If it does not find a match, it discards the route or update message. This means that route maps end with an implicit deny entry. To permit all non-matching routes or update messages, end your route map with an entry that has an action of **permit** and no match clause.

Examples

To enter route-map mode for entry 1 of the route map called "route1", and then add a match and set clause to it, use the commands:

```
awplus# configure terminal
awplus(config)# route-map route1 permit 1
awplus(config-route-map)# match as-path 60
awplus(config-route-map)# set weight 70
```

To enter route-map mode for entry 2 of the route map called "route1", and then add a match and set clause to it, use the commands:

```
awplus# configure terminal
awplus(config)# route-map route1 permit 2
awplus(config-route-map)# match interface vlan2
awplus(config-route-map)# set metric 20
```

Note how the prompt changes when you go into route map configuration mode.

To make the device process non-matching routes instead of discarding them, add a command like the following one:

```
awplus(config)# route-map route1 permit 100
```

Related commands

For BGP:

show route-map

bgp dampening

neighbor default-originate

neighbor route-map

neighbor unsuppress-map

network (BGP and BGP4+)

redistribute (into BGP or BGP4+)

show ip bgp route-map (BGP only)

For OSPF:

distribute-list (OSPF)

default-information originate

redistribute (OSPF)

For RIP:

redistribute (RIP)

set as-path

Overview Use this command to add an AS path set clause to a route map entry.

When a BGP update message matches the route map entry, the device prepends the specified Autonomous System Number (ASN) or ASNs to the update's AS path attribute.

The AS path attribute is a list of the autonomous systems through which the announcement for the prefix has passed. As prefixes pass between autonomous systems, each autonomous system adds its ASN to the beginning of the list. This means that the AS path attribute can be used to make routing decisions.

Use the **no** variant of this command to remove the set clause.

Syntax

```
set as-path prepend <1-65535> [<1-65535>]...
no set as-path prepend [<1-65535> [<1-65535>]...]
```

Parameter	Description
`prepend`	Prepends the autonomous system path.
<1-65535>	The number to prepend to the AS path. If you specify multiple ASNs, separate them with spaces.

Mode Route-map mode

Usage notes Use the **set as-path** command to specify an autonomous system path. By specifying the length of the AS-Path, the device influences the best path selection by a neighbor. Use the `prepend` parameter with this command to prepend an AS path string to routes increasing the AS path length.

This command is valid for BGP update messages only.

Example To use entry `3` of the route map called `myroute` to prepend ASN `8` and `24` to the AS path of matching update messages, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# set as-path prepend 8 24
```

Related commands

match as-path

route-map

show route-map

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

set community

Overview Use this command to add a community set clause to a route map entry.

When a BGP update message matches the route map entry, the device takes one of the following actions:

- changes the update's community attribute to the specified value or values, or
- adds the specified community value or values to the update's community attribute, if you specify the **additive** parameter after specifying another parameter. or
- removes the community attribute from the update, if you specify the **none** parameter

Use the **no** variant of this command to remove the set clause.

Syntax

```
set community {[<1-65535>][AA:NN] [internet] [local-AS]
[no-advertise] [no-export] [additive]}
```

```
no set community {[AA:NN] [internet] [local-AS] [no-advertise]
[no-export] [additive]}
```

```
set community none
```

```
no set community none
```

Parameter	Description
<1-65535>	The AS number of the community as an integer not in AA:NN format.
AA:NN	The Autonomous System (AS) number of the community, in AA:NN format. AS numbers are assigned to the regional registries by the IANA (www.iana.org) and can be obtained from the registry in your region. AA and NN are both integers from 1 to 65535. AA is the AS number; NN is a value chosen by the ASN administrator.
`local-AS`	The community of routes that must not be advertised to external BGP peers (this includes peers in other members' Autonomous Systems inside a BGP confederation).
`internet`	The community of routes that can be advertised to all BGP peers.
`no-advertise`	The community of routes that must not be advertised to other BGP peers.
`no-export`	The community of routes that must not be advertised outside a BGP confederation boundary (a standalone Autonomous System that is not part of a confederation should be considered a confederation itself).

Parameter	Description
`none`	The device removes the community attribute from matching update messages.
`additive`	The device adds the specified community value to the update message's community attribute, instead of replacing the existing attribute. By default this parameter is not included, so the device replaces the existing attribute.

Mode Route-map Configuration

Usage notes This command is valid for BGP update messages only.

Examples To use entry `3` of the route map called `rmap1` to put matching routes into the no-advertise community, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community no-advertise
```

To use entry `3` of the route map called `rmap1` to put matching routes into several communities, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community 10:01 23:34 12:14
no-export
```

To use entry `3` of the route map called `rmap1` to put matching routes into a single AS community numbered `16384`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community 16384 no-export
```

Related commands

match community

route-map

set aggregator

set comm-list delete

set extcommunity

show route-map

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 (BGP4+ only)

Overview Use this command to display BGP4+ network information for a specified IPv6 address.

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

Syntax

```
show bgp ipv6 <ipv6-addr>
```

Parameter	Description
<ipv6-addr>	Specifies the IPv6 address, entered in hexadecimal in the format X:X::X:X.

Mode User Exec and Privileged Exec

Example

```
awplus# show bgp ipv6 2001:0db8:010d::1
```

Related commands show bgp ipv6 longer-prefixes (BGP4+ only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 community (BGP4+ only)

Overview Use this command to display routes that match specified communities within an IPv6 environment. Use the show ip bgp community (BGP only) command within an IPv4 environment.

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

You may use any combination and repetition of parameters listed in the *<type>* placeholder.

Syntax

```
show bgp ipv6 community [<type>] [exact-match]
```

Parameter		Description
<type>	{[*AA:NN*][local-AS][no-advertise][no-export]}	
	AA:NN	Specifies the Autonomous System (AS) community number, in AA:NN format.
	local-AS	Do not send outside local Autonomous Systems (well-known community).
	no-advertise	Do not advertise to any peer (well-known community).
	no-export	Do not export to next AS (well-known community).
exact-match	Specifies that the exact match of the communities is displayed. This optional parameter cannot be repeated.	

Mode User Exec and Privileged Exec

Examples Note that the AS numbers shown are examples only.

```
awplus# show bgp ipv6 community 64497:64499 exact-match
```

```
awplus# show bgp ipv6 community 64497:64499 64500:64501
exact-match
```

```
awplus# show bgp ipv6 community 64497:64499 64500:64501
64510:64511no-advertise
```

```
awplus# show bgp ipv6 community no-advertise
no-advertiseno-advertise exact-match
```

```
awplus# show bgp ipv6 community no-export 64510:64511
no-advertise local-AS no-export
```

```
awplus# show bgp ipv6 community no-export 64510:64511
no-advertise 64497:64499 64500:64501 no-export
```

```
awplus# show bgp ipv6 community no-export 64497:64499
no-advertise local-AS no-export
```

Related commands

show ip bgp community (BGP only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 community-list (BGP4+ only)

Overview Use this command to display routes that match the given community-list within an IPv6 environment. Use the show ip bgp community-list (BGP only) command within an IPv4 environment.

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

Syntax

```
show bgp ipv6 community-list <listname> [exact-match]
```

Parameter	Description
`<listname>`	Specifies the community list name.
`exact-match`	Displays only routes that have exactly the same specified communities.

Mode User Exec and Privileged Exec

Example

```
awplus# show bgp ipv6 community-list mylist exact-match
```

Related commands show ip bgp community-list (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 dampening (BGP4+ only)

Overview Use this command to show dampened routes from a BGP4+ instance within an IPv6 environment. Use the show ip bgp dampening (BGP only) command to show dampened routes from a BGP instance within an IPv4 environment.

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

Syntax

```
show bgp ipv6 dampening
{dampened-paths|flap-statistics|parameters}
```

Parameter	Description
`dampened-paths`	Display paths suppressed due to dampening.
`flap-statistics`	Display flap statistics of routes.
`parameters`	Display details of configured dampening parameters.

Mode User Exec and Privileged Exec

Usage notes Enable BGP4+ dampening to maintain dampened-path information in memory.

Examples

```
awplus# show bgp ipv6 dampening dampened-path
awplus# show bgp ipv6 dampening flap-statistics
awplus# show bgp ipv6 dampening parameter
```

Related commands show ip bgp dampening (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 filter-list (BGP4+ only)

Overview Use this command to display routes conforming to the filter-list within an IPv6 environment. Use the show ip bgp filter-list (BGP only) command to display routes conforming to the filter-list within an IPv4 environment.

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

Syntax

```
show bgp ipv6 filter-list <listname>
```

Parameter	Description
<listname>	Specifies the regular-expression access list name.

Mode User Exec and Privileged Exec

Example

```
awplus# show bgp ipv6 filter-list mylist
```

Related commands show ip bgp filter-list (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 inconsistent-as (BGP4+ only)

Overview Use this command to display routes with inconsistent AS Paths within an IPv6 environment. Use the show ip bgp inconsistent-as (BGP only) command to display routes with inconsistent AS paths within an IPv4 environment.

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

Syntax

```
show bgp ipv6 inconsistent-as
```

Mode User Exec and Privileged Exec

Example

```
awplus# show bgp ipv6 inconsistent-as
```

Related commands show ip bgp inconsistent-as (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 longer-prefixes (BGP4+ only)

Overview Use this command to display the route of the local BGP4+ routing table for a specific prefix with a specific mask or for any prefix having a longer mask than the one specified.

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

Syntax

```
show bgp ipv6 <ipv6-addr/prefix-length> longer-prefixes
```

Parameter	Description
<ipv6-addr/prefix-length>	Specifies the IPv6 address with prefix length. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.

Mode User Exec and Privileged Exec

Example

```
awplus# show bgp ipv6 2001:0db8::/64 longer-prefixes
```

Related commands show bgp ipv6 (BGP4+ only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 neighbors (BGP4+ only)

Overview Use this command to display detailed information on peering connections to all BGP4+ neighbors within an IPv6 environment.

Use the show ip bgp neighbors (BGP only) command to display detailed information on peering connections to all BGP neighbors within an IPv4 environment.

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

Syntax

```
show bgp ipv6 neighbors [<ipv6-addr> [advertised-routes|
received prefix-filter|received-routes|routes]]
```

Parameter	Description
<ipv6-addr>	Specifies the IPv6 address, entered in hexadecimal in the format X:X::X:X.
`advertised-routes`	Displays the routes advertised to a BGP4+ neighbor.
`received prefix-filter`	Displays received prefix-list filters.
`received-routes`	Displays the received routes from the neighbor. To display all the received routes from the neighbor, configure the BGP4+ soft reconfigure first.
`routes`	Displays all accepted routes learned from neighbors.

Mode User Exec and Privileged Exec

Examples [BGP4+]

```
awplus# show bgp ipv6 neighbors 2001:0db8:010d::1
advertised-routes
```

```
awplus# show bgp ipv6 neighbors 2001:0db8:010d::1 received
prefix-filter
```

```
awplus# show bgp ipv6 neighbors 2001:0db8:010d::1
received-routes
```

```
awplus# show bgp ipv6 neighbors 2001:0db8:010d::1 routes
```

Output Figure 30-4: Example output from **show bgp ipv6 neighbors** 2001:db8:b::1

```
awplus#show bgp ipv6 neighbors 2001:db8:b::1
BGP neighbor is 2001:db8:b::1, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 2.2.2.1
  BGP state = Established, up for 01:03:26
  Last read 01:03:26, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Octet ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 157 messages, 0 notifications, 0 in queue
  Sent 228 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Update source is lo
For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

For address family: IPv6 Unicast
  BGP table version 66, neighbor version 66
  Index 2, Offset 0, Mask 0x4
  AF-dependant capabilities:
    Graceful restart: advertised, received

  Community attribute sent to this neighbor (both)
  Default information originate, default sent
  Inbound path policy configured
  Incoming update prefix filter list is *BGP_FILTER_LIST
  Route map for incoming advertisements is *BGP_LOCAL_PREF_MAP
  8 accepted prefixes
  8 announced prefixes

Connections established 1; dropped 0
Graceful-restart Status:
  Remote restart-time is 90 sec

  External BGP neighbor may be up to 2 hops away.
Local host: 2001:db8:a::1, Local port: 179
Foreign host: 2001:db8:b::1, Foreign port: 50672
Nexthop: 1.1.1.1
Nexthop global: 2001:db8:a::1
Nexthop local: ::
BGP connection: non shared network
```

If available the following is shown:

- Session information
  - Neighbor address, ASN information and if the link is external or internal
  - BGP version and status
  - Neighbor capabilities for the BGP session
  - Number of messages transmitted and received
- IPv6 unicast address family information
  - BGP4+ table version
  - IPv6 Address Family dependent capabilities
  - IPv6 Communities
  - IPv6 Route filters for ingress and egress updates
  - Number of announced and accepted IPv6 prefixes
- Connection information
  - Connection counters
  - Graceful restart timer
  - Hop count to the peer
  - Next hop information
  - Local and external port numbers

Related commands show ip bgp neighbors (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 paths (BGP4+ only)

Overview Use this command to display BGP4+ path information within an IPv6 environment. Use the show ip bgp paths (BGP only) command to display BGP path information within an IPv4 environment.

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

Syntax

```
show bgp ipv6 paths
```

Mode User Exec and Privileged Exec

Example

```
awplus# show bgp ipv6 paths
```

Related commands show ip bgp paths (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 prefix-list (BGP4+ only)

Overview Use this command to display routes matching the prefix-list within an IPv6 environment. Use the show ip bgp prefix-list (BGP only) command to display routes matching the prefix-list within an IPv4 environment.

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

Syntax

```
show bgp ipv6 prefix-list <list>
```

Parameter	Description
<list>	Specifies the name of the IPv6 prefix list.

Mode User Exec and Privileged Exec

Example

```
awplus# show bgp ipv6 prefix-list mylist
```

Related commands show ip bgp prefix-list (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 quote-regexp (BGP4+ only)

Overview Use this command to display routes matching the AS path regular expression within an IPv6 environment. Use the show ip bgp quote-regexp (BGP only) command to display routes matching the AS path regular expression within an IPv4 environment.

Note that you must use quotes to enclose the regular expression with this command. Use the regular expressions listed below with the <*expression*> parameter:

Symbol	Character	Meaning
^	Caret	Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign	Used to match the end of the input string.
.	Period	Used to match a single character (white spaces included).
*	Asterisk	Used to match none or more sequences of a pattern.
+	Plus sign	Used to match one or more sequences of a pattern.
?	Question mark	Used to match none or one occurrence of a pattern.
_	Underscore	Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.
[ ]	Brackets	Specifies a range of single-characters.
-	Hyphen	Separates the end points of a range.

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

Syntax
```
show bgp ipv6 quote-regexp <expression>
```

Mode User Exec and Privileged Exec

Example
```
awplus# show bgp ipv6 quote-regexp myexpression
```

Related commands show ip bgp quote-regexp (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 regexp (BGP4+ only)

Overview Use this command to display routes matching the AS path regular expression within an IPv6 environment. Use the show ip bgp regexp (BGP only) command to display routes matching the AS path regular expression within an IPv4 environment.

Use the regular expressions listed below with the <*expression*> parameter:

Symbol	Character	Meaning
^	Caret	Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign	Used to match the end of the input string.
.	Period	Used to match a single character (white spaces included).
*	Asterisk	Used to match none or more sequences of a pattern.
+	Plus sign	Used to match one or more sequences of a pattern.
?	Question mark	Used to match none or one occurrence of a pattern.
_	Underscore	Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.
[ ]	Brackets	Specifies a range of single-characters.
-	Hyphen	Separates the end points of a range.

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

Syntax

```
show bgp ipv6 regexp <expression>
```

Parameter	Description
<*expression*>	Specifies a regular-expression to match the BGP4+ AS paths.

Mode User Exec and Privileged Exec

Example

```
awplus# show bgp ipv6 regexp myexpression
```

Related commands show ip bgp regexp (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 route-map (BGP4+ only)

Overview Use this command to display BGP4+ routes that match the specified route-map within an IPv6 environment. Use the show ip bgp route-map (BGP only) command to display BGP routes that match the specified route-map within an IPv4 environment.

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

Syntax

```
show bgp ipv6 route-map <route-map>
```

Parameter	Description
<route-map>	Specifies a route-map that is matched.

Mode User Exec and Privileged Exec

Example To show routes that match the route-map `myRouteMap`, use the command:

```
awplus# show bgp ipv6 route-map myRouteMap
```

Related commands show ip bgp route-map (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp ipv6 summary (BGP4+ only)

Overview Use this command to display a summary of a BGP4+ neighbor status within an IPv6 environment. Use the show ip bgp summary (BGP only) command to display a summary of a BGP neighbor status within an IPv4 environment.

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

Syntax

```
show bgp ipv6 summary
```

Mode User Exec and Privileged Exec

Example

```
awplus# show bgp ipv6 summary
```

Output Figure 30-5: Example output from the **show ip bgp summary** command

```
awplus>show ip bgp summary

BGP router identifier 1.0.0.1, local AS number 65541
BGP table version is 12
4 BGP AS-PATH entries
0 BGP community entries

Neighbor           V         AS   MsgRc  MsgSnt TblVer InOutQ Up/Down   State/PfxRcd
2001:0db8:cccc::1  4      65544      20      24     11 0/0    00:07:19          1
2001:0db8:dddd::1  4      65545       0       0      0 0/0    never         Active
2001:0db8:eeee::1  4      65542      34      40      0 0/0    00:00:04      Active
2001:0db8:ffff::1  4      65543      29      32     11 0/0    00:07:03         13

Number of neighbors 4
```

The Up/Down column in this output is a timer that shows:

- "never" if the peer session has never been established
- The up time, if the peer session is currently up
- The down time, if the peer session is currently down.

In the example above, the session with 2001:0db8:eeee::1 has been down for 4 seconds, and the session with 2001:0db8:dddd::1 has never been established.

Related commands show ip bgp summary (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp memory maxallocation (BGP only)

Overview This command displays the maximum percentage of total memory that is allocated to BGP processes.

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

Syntax

```
show bgp memory maxallocation
```

Mode User Exec and Privileged Exec

Example To display the maximum amount of memory allocated for BGP processes, use the command:

```
awplus# show bgp memory maxallocation
```

Output Figure 30-6: Example output from the **show bgp memory maxallocation** command

```
BGP maximum RAM allocation is 100%
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp nexthop-tracking (BGP only)

Overview Use this command to display BGP next hop tracking status.

Syntax
```
show bgp nexthop-tracking
```

Mode User Exec and Privileged Exec

Example To display BGP next hop tracking status, use the command:

```
awplus# show bgp nexthop-tracking
```

Related commands bgp nexthop-trigger-count

show bgp nexthop-tree-details (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show bgp nexthop-tree-details (BGP only)

Overview Use this command to display BGP next hop tree details.

Syntax

```
show bgp nexthop-tree-details
```

Mode User Exec and Privileged Exec

Example To display BGP next hop tree details, use the command:

```
awplus# show bgp nexthop-tree-details
```

Related commands show bgp nexthop-tracking (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show debugging bgp (BGP only)

Overview Use this command to see what debugging is turned on for BGP.

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

Syntax

```
show debugging bgp
```

Mode User Exec and Privileged Exec

Example

```
awplus# show debugging bgp
```

Output Figure 30-7: Example output from the **show debugging bgp** command

```
BGP debugging status:
  BGP debugging is on
  BGP events debugging is on
  BGP updates debugging is on
  BGP fsm debugging is on
```

Related commands debug bgp (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp (BGP only)

Overview Use this command to display BGP network information.

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

Syntax

```
show ip bgp [<ip-addr>|<ip-addr/m>]
```

Parameter	Description
<ip-addr> *<ip-addr/m>*	Specifies the IPv4 address and the optional prefix mask length.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp 10.10.1.34/24
```

Output Figure 30-8: Example output from the **show ip bgp** command

```
BGP table version is 7, local router ID is 80.80.80.80
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight
Path
S>i10.70.0.0/24     192.10.23.67             0    100      0 ?
S>i30.30.30.30/32   192.10.23.67             0    100      0 ?
S>i63.63.63.1/32    192.10.23.67             0    100      0 ?
S>i67.67.67.67/32   192.10.23.67             0    100      0 ?
S>i172.22.10.0/24   192.10.23.67             0    100      0 ?
S>i192.10.21.0      192.10.23.67             0    100      0 ?
S>i192.10.23.0      192.10.23.67             0    100      0 ?

Total number of prefixes 7
```

Related commands neighbor remove-private-AS (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp attribute-info (BGP only)

Overview Use this command to show internal attribute hash information.

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

Syntax

```
show ip bgp attribute-info
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp attribute-info
```

Output Figure 30-9: Example output from the **show ip bgp attribute-info** command

```
attr[1] nexthop 0.0.0.0
attr[1] nexthop 10.10.10.10
attr[1] nexthop 10.10.10.50
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp cidr-only (BGP only)

Overview Use this command to display routes with non-natural network masks.

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

Syntax

```
show ip bgp cidr-only
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp cidr-only
```

Output Figure 30-10: Example output from the **show ip bgp cidr-only** command

```
BGP table version is 0, local router ID is 10.10.10.50

Status codes: s suppressed, d damped, h history, p stale, *
valid, > best, i - internal

Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 3.3.3.0/24       10.10.10.10                              0 11 i
*> 6.6.6.0/24       0.0.0.0                              32768 i

Total number of prefixes 2
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp community (BGP only)

Overview Use this command to display routes that match specified communities from a BGP instance within an IPv4 environment. Use the show bgp ipv6 community (BGP4+ only) command within an IPv6 environment.

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

You may use any combination and repetition of parameters listed in the *<type>* placeholder.

Syntax `show ip bgp community [<type>] [exact-match]`

Parameter		Description
`<type>`	{[*AA:NN*][local-AS][no-advertise][no-export]}	
	AA:NN	Specifies the Autonomous System (AS) community number, in AA:NN format.
	local-AS	Do not send outside local Autonomous Systems (well-known community).
	no-advertise	Do not advertise to any peer (well-known community).
	no-export	Do not export to next AS (well-known community).
exact-match	Specifies that the exact match of the communities is displayed. This optional parameter cannot be repeated.	

Mode User Exec and Privileged Exec

Examples Note that the AS numbers shown are examples only.

```
awplus# show ip bgp community 64497:64499 exact-match
```

```
awplus# show ip bgp community 64497:64499 64500:64501
exact-match
```

```
awplus# show ip bgp community 64497:64499 64500:64501
64510:64511no-advertise
```

```
awplus# show ip bgp community no-advertise
no-advertiseno-advertise exact-match
```

```
awplus# show ip bgp community no-export 64510:64511
no-advertise local-AS no-export
```

```
awplus# show ip bgp community no-export 64510:64511
no-advertise 64497:64499 64500:64501 no-export
```

```
awplus# show ip bgp community no-export 64497:64499
no-advertise local-AS no-export
```

Related commands

set community

show bgp ipv6 community (BGP4+ only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp community-info (BGP only)

Overview Use this command to list all BGP community information.

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

Syntax

```
show ip bgp community-info
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp community-info
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp community-list (BGP only)

Overview Use this command to display routes that match the given community-list from a BGP instance within an IPv4 environment. Use the show bgp ipv6 community-list (BGP4+ only) command within an IPv6 environment.

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

Syntax

```
show ip bgp community-list <listname> [exact-match]
```

Parameter	Description
`<listname>`	Specifies the community list name.
`exact-match`	Displays only routes that have exactly the same specified communities.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp community-list mylist exact-match
```

Related commands show bgp ipv6 community-list (BGP4+ only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp dampening (BGP only)

Overview Use this command to show dampened routes from a BGP instance within an IPv4 environment. Use the show bgp ipv6 dampening (BGP4+ only) command within an IPv6 environment.

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

Syntax

```
show ip bgp dampening
{dampened-paths|flap-statistics|parameters}
```

Parameter	Description
`dampened-paths`	Display paths suppressed due to dampening.
`flap-statistics`	Display flap statistics of routes.
`parameters`	Display details of configured dampening parameters.

Mode User Exec and Privileged Exec

Usage notes Enable BGP dampening to maintain dampened-path information in memory.

Examples

```
awplus# show ip bgp dampening dampened-paths
```

Output Figure 30-11: Example output from the **show ip bgp dampening** command

```
dampening 15 750 2000 60 15
 Reachability Half-Life time    : 15 min
 Reuse penalty                  : 750
 Suppress penalty               : 2000
 Max suppress time              : 60 min
 Un-reachability Half-Life time : 15 min
 Max penalty (ceil)             : 11999
 Min penalty (floor)            : 375
```

The following example output shows that the internal route (`i`), has flapped 3 times and is now categorized as history (`h`).

Figure 30-12: Example output from the **show ip bgp dampening flap-statistics** command

```
awplus# show ip bgp dampening flap-statistics
BGP table version is 1, local router ID is 30.30.30.77
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,S
Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From            Flaps  Duration  Reuse    Path
 hi1.1.1.0/24       10.100.0.62        3   00:01:20            i
```

The following example output shows a dampened route in the `1.1.1.0/24` network.

Figure 30-13: Example output from the **show ip bgp dampening dampened-path** command

```
awplus# show ip bgp dampening dampened-paths
BGP table version is 1, local router ID is 30.30.30.77
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,S
Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network            From              Reuse     Path
 di 1.1.1.0/24       10.100.0.62        00:35:10     i

Total number of prefixes 1
```

Related commands

show bgp ipv6 dampening (BGP4+ only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp filter-list (BGP only)

Overview Use this command to display routes conforming to the filter-list within an IPv4 environment. Use the show bgp ipv6 filter-list (BGP4+ only) command to display routes conforming to the filter-list within an IPv6 environment

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

Syntax

```
show ip bgp filter-list <listname>
```

Parameter	Description
<listname>	Specifies the regular-expression access list name.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp filter-list mylist
```

Related commands show bgp ipv6 filter-list (BGP4+ only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp inconsistent-as (BGP only)

Overview Use this command to display routes with inconsistent AS Paths within an IPv4 environment. Use the show bgp ipv6 inconsistent-as (BGP4+ only) command to display routes with inconsistent AS paths within an IPv6 environment.

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

Syntax
```
show ip bgp inconsistent-as
```

Mode User Exec and Privileged Exec

Example
```
awplus# show ip bgp inconsistent-as
```

Related commands show bgp ipv6 inconsistent-as (BGP4+ only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp longer-prefixes (BGP only)

Overview Use this command to display the route of the local BGP routing table for a specific prefix with a specific mask, or for any prefix having a longer mask than the one specified.

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

Syntax

```
show ip bgp <ip-address/m> longer-prefixes
```

Parameter	Description
<ip-address/m>	Neighbor's IP address and subnet mask, entered in the form A.B.C.D/M, where M is the subnet mask length.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp 10.10.0.10/24 longer-prefixes
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp neighbors (BGP only)

Overview Use this command to display detailed information on peering connections to all BGP neighbors within an IPv4 environment.

Use the show bgp ipv6 neighbors (BGP4+ only) command to display detailed information on peering connections to all BGP4+ neighbors within an IPv6 environment.

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

Syntax [BGP]

```
show ip bgp neighbors [<ipv4-addr> [advertised-routes|received
prefix-filter|received-routes|routes]]
```

Parameter	Description
<ipv4-addr>	The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.
`advertised-routes`	Displays the routes advertised to a BGP neighbor.
`received prefix-filter`	Displays the received prefix-list filters.
`received-routes`	Displays the received routes from the neighbor. To display all the received routes from the neighbor, configure the BGP soft reconfigure first.
`routes`	Displays all accepted routes learned from neighbors.

Mode [BGP] User Exec and Privileged Exec

Examples [BGP]

```
awplus# show ip bgp neighbors 10.10.10.72 advertised-routes
awplus# show ip bgp neighbors 10.10.10.72 received
prefix-filter
awplus# show ip bgp neighbors 10.10.10.72 received-routes
awplus# show ip bgp neighbors 10.10.10.72 routes
```

Output Figure 30-14: Example output from **show ip bgp neighbors 10.10.10.72**

```
awplus#show ip bgp neighbors 10.10.10.72
BGP neighbor is 10.10.10.72, remote AS 100, local AS 100, internal
 link
 Member of peer-group group1 for session parameters
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
  Last read         , hold time is 90, keepalive interval is 30 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  group1 peer-group member
  NEXT_HOP is always this router
  0 accepted prefixes
  0 announced prefixes

 Connections established 0; dropped 0
Next connect timer due in 33 seconds
```

If available the following is shown:

- Session information
  - Neighbor address, ASN information and if the link is external or internal
  - BGP version and status
  - Neighbor capabilities for the BGP session
  - Number of messages transmitted and received
- IPv4 unicast address family information
  - BGP table version
  - IPv4 Address Family dependent capabilities
  - IPv4 Communities
  - IPv4 Route filters for ingress and egress updates
  - Number of announced and accepted IPv4 prefixes
- Connection information
  - Connection counters
  - Graceful restart timer
  - Hop count to the peer
  - Next hop information
  - Local and external port numbers

Related commands

show bgp ipv6 neighbors (BGP4+ only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp neighbors connection-retrytime (BGP only)

Overview Use this command to display the configured connection-retrytime value of the peer at the session establishment time with the neighbor.

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

Syntax

```
show ip bgp neighbors <ipv4-addr> connection-retrytime
```

Parameter	Description
<ipv4-addr>	The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp neighbors 10.11.4.26 connection-retrytime
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp neighbors hold-time (BGP only)

Overview Use this command to display the configured holdtime value of the peer at the session establishment time with the neighbor.

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

Syntax

```
show ip bgp neighbors <ipv4-addr> hold-time
```

Parameter	Description
<ipv4-addr>	The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

Default The holdtime timer default is 90 seconds as per RFC 4271. Holdtime is keepalive * 3.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip bgp neighbors 10.11.4.26 hold-time
```

Related commands

neighbor timers

show ip bgp neighbors keepalive-interval (BGP only)

timers (BGP)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp neighbors keepalive (BGP only)

Overview Use this command to display the number of keepalive messages sent to the neighbor from the peer throughout the session.

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

Syntax

```
show ip bgp neighbors <ipv4-addr> keepalive
```

Parameter	Description
<ipv4-addr>	The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip bgp neighbors 10.11.4.26 keepalive
```

Related commands show ip bgp neighbors keepalive-interval (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp neighbors keepalive-interval (BGP only)

Overview Use this command to display the configured keepalive-interval value of the peer at the session establishment time with the neighbor.

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

Syntax

```
show ip bgp neighbors <ipv4-addr> keepalive-interval
```

Parameter	Description
<ipv4-addr>	The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

Default The keepalive timer default is 60 seconds as per RFC 4271. Keepalive is holdtime / 3.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip bgp neighbors 10.11.4.26 keepalive-interval
```

Related commands

neighbor timers

show ip bgp neighbors hold-time (BGP only)

timers (BGP)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp neighbors notification (BGP only)

Overview Use this command to display the number of notification messages sent to the neighbor from the peer throughout the session.

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

Syntax

```
show ip bgp neighbors <ipv4-addr> notification
```

Parameter	Description
<ipv4-addr>	The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp neighbors 10.11.4.26 notification
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp neighbors open (BGP only)

Overview Use this command to display the number of open messages sent to the neighbor from the peer throughout the session.

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

Syntax

```
show ip bgp neighbors <ipv4-addr> open
```

Parameter	Description
<ipv4-addr>	The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp neighbors 10.11.4.26 open
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp neighbors rcvd-msgs (BGP only)

Overview Use this command to display the number of messages received by the neighbor from the peer throughout the session.

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

Syntax

```
show ip bgp neighbors <ipv4-addr> rcvd-msgs
```

Parameter	Description
<ipv4-addr>	The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp neighbors 10.11.4.26 rcvd-msgs
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp neighbors sent-msgs (BGP only)

Overview Use this command to display the number of messages sent to the neighbor from the peer throughout the session.

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

Syntax

```
show ip bgp neighbors <ipv4-addr> sent-msgs
```

Parameter	Description
<ipv4-addr>	The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp neighbors 10.11.4.26 sent-msgs
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp neighbors update (BGP only)

Overview Use this command to display the number of update messages sent to the neighbor from the peer throughout the session.

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

Syntax

```
show ip bgp neighbors <ipv4-addr> update
```

Parameter	Description
<ipv4-addr>	The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp neighbors 10.11.4.26 update
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp paths (BGP only)

Overview Use this command to display BGP4 path information within an IPv4 environment. Use the show bgp ipv6 paths (BGP4+ only) command to display BGP4+ path information within an IPv4 environment.

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

Syntax

```
show ip bgp paths
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp paths
```

Related commands show bgp ipv6 paths (BGP4+ only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp prefix-list (BGP only)

Overview Use this command to display routes matching the prefix-list within an IPv4 environment. Use the show bgp ipv6 prefix-list (BGP4+ only) command to display routes matching the prefix-list within an IPv6 environment.

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

Syntax

```
show ip bgp prefix-list <list>
```

Parameter	Description
<list>	Specifies the name of the IP prefix list.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip bgp prefix-list mylist
```

Related commands show bgp ipv6 prefix-list (BGP4+ only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp quote-regexp (BGP only)

Overview Use this command to display routes matching the AS path regular expression within an IPv4 environment. Use the show bgp ipv6 quote-regexp (BGP4+ only) command to display routes matching the AS path regular expression within an IPv6 environment.

Note that you must use quotes to enclose the regular expression with this command. Use the regular expressions listed below with the <*expression*> parameter:

Symbol	Character	Meaning
^	Caret	Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign	Used to match the end of the input string.
.	Period	Used to match a single character (white spaces included).
*	Asterisk	Used to match none or more sequences of a pattern.
+	Plus sign	Used to match one or more sequences of a pattern.
?	Question mark	Used to match none or one occurrence of a pattern.
_	Underscore	Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.
[ ]	Brackets	Specifies a range of single-characters.
-	Hyphen	Separates the end points of a range.

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

Syntax

```
show ip bgp quote-regexp <expression>
```

Parameter	Description
<*expression*>	Specifies a regular-expression to match the BGP AS paths.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip bgp quote-regexp myexpression
```

Related commands show bgp ipv6 quote-regexp (BGP4+ only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp regexp (BGP only)

Overview Use this command to display routes matching the AS path regular expression within an IPv4 environment. Use the show bgp ipv6 regexp (BGP4+ only) command to display routes matching the AS path regular expression within an IPv6 environment.

Use the regular expressions listed below with the <*expression*> parameter:

Symbol	Character	Meaning
^	Caret	Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign	Used to match the end of the input string.
.	Period	Used to match a single character (white spaces included).
*	Asterisk	Used to match none or more sequences of a pattern.
+	Plus sign	Used to match one or more sequences of a pattern.
?	Question mark	Used to match none or one occurrence of a pattern.
_	Underscore	Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.
[ ]	Brackets	Specifies a range of single-characters.
-	Hyphen	Separates the end points of a range.

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

Syntax

```
show ip bgp regexp <expression>
```

Parameter	Description
<*expression*>	Specifies a regular-expression to match the BGP AS paths.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip bgp regexp myexpression
```

Related commands show bgp ipv6 regexp (BGP4+ only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp route-map (BGP only)

Overview Use this command to display BGP routes that match the specified route-map within an IPv4 environment. Use the show bgp ipv6 route-map (BGP4+ only) command to display BGP4+ routes that match the specified route-map within an IPv6 environment.

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

Syntax

```
show ip bgp route-map <route-map>
```

Parameter	Description
<route-map>	Specifies a route-map that is matched.

Mode User Exec and Privileged Exec

Examples To show routes that match the route-map `myRouteMap`, use the command:

```
awplus# show ip bgp route-map myRouteMap
```

Related commands show bgp ipv6 route-map (BGP4+ only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp scan (BGP only)

Overview Use this command to display BGP scan status.

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

Syntax

```
show ip bgp scan
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip bgp scan
```

Output Figure 30-15: Example output from the **show ip bgp scan** command

```
BGP scan is running
BGP scan interval is 60
BGP instance : AS is 11,DEFAULT
Current BGP nexthop cache:
BGP connected route:
 10.10.10.0/24
 10.10.11.0/24
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip bgp summary (BGP only)

Overview Use this command to display a summary of a BGP neighbor status within an IPv4 environment. Use the show bgp ipv6 summary (BGP4+ only) command to display a summary of BGP4+ neighbors.

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

Syntax

```
show ip bgp summary
```

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip bgp summary
```

Output Figure 30-16: Example output from the **show ip bgp summary** command

```
awplus>show ip bgp summary

BGP router identifier 1.0.0.1, local AS number 65541
BGP table version is 12
4 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS   MsgRc  MsgSnt TblVer InOutQ Up/Down   State/PfxRcd
192.168.3.2     4      65544      20      24     11 0/0    00:07:19          1
192.168.4.2     4      65545       0       0      0 0/0    never         Active
192.168.11.2    4      65542      34      40      0 0/0    00:00:04      Active
192.168.21.2    4      65543      29      32     11 0/0    00:07:03         13

Number of neighbors 4
```

The Up/Down column in this output is a timer that shows:

- "never" if the peer session has never been established
- The up time, if the peer session is currently up
- The down time, if the peer session is currently down.

In the example above, the session with 192.168.11.2 has been down for 4 seconds, and the session with 192.168.4.2 has never been established.

Related commands show bgp ipv6 summary (BGP4+ only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip community-list

Overview Use this command to display routes that match a specified community-list name or number.

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

Syntax

```
show ip community-list [<listnumber>|<listname>]
```

Parameter	Description
<listnumber>	Specifies the community list number in the range <1-199> as specified by a previously issued **ip community-list** command.
<listname>	Specifies the community list name as specified by a previously issued ip community-list command.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip community-list mylist
awplus# show ip community-list 99
```

Related commands

ip community-list

ip community-list expanded

ip community-list standard

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip extcommunity-list

Overview Use this command to display a configured extcommunity-list.

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

Syntax

```
show ip extcommunity-list [<1-199>|<extcommunity-listname>]
```

Parameter	Description
<1-199>	Extcommunity-list number
<extcommunity-listname>	Extcommunity-list name

Mode User Exec and Privileged Exec

Example

```
awplus# show ip extcommunity-list 33
```

Related commands

ip extcommunity-list expanded

ip extcommunity-list standard

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show ip prefix-list

Overview Use this command to display the IPv4 prefix-list entries.

Note that this command is valid for RIP and BGP routing protocols only.

Syntax

```
show ip prefix-list [<name>|detail|summary]
```

Parameter	Description
<name>	Specify the name of a prefix list in this placeholder.
`detail`	Specify this parameter to show detailed output for all IPv4 prefix lists.
`summary`	Specify this parameter to show summary output for all IPv4 prefix lists.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip prefix-list
awplus# show ip prefix-list 10.10.0.98/8
awplus# show ip prefix-list detail
```

Related commands ip prefix-list

show ipv6 prefix-list

Overview Use this command to display the prefix-list entries.

Note that this command is valid for RIPng and BGP4+ routing protocols only.

Syntax

```
show ipv6 prefix-list [<name>|detail|summary]
```

Parameter	Description
<name>	Specify the name of an individual IPv6 prefix list.
`detail`	Specify this parameter to show detailed output for all IPv6 prefix lists.
`summary`	Specify this parameter to show summary output for all IPv6 prefix lists.

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 prefix-list
awplus# show ipv6 prefix-list 10.10.0.98/8
awplus# show ipv6 prefix-list detail
```

Related commands ipv6 prefix-list

show ip protocols bgp (BGP only)

Overview Use this command to display BGP process parameters and statistics.

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

Syntax

```
show ip protocols bgp
```

Mode User Exec and Privileged Exec

Example To display BGP process parameters and statistics, use the command:

```
awplus# show ip protocols bgp
```

Output Figure 30-17: Example output from the **show ip protocols bgp** command

```
Routing Protocol is "bgp 100"
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Default local-preference applied to incoming route is 100
  Redistributing:
  Neighbor(s):
  Address AddressFamily FiltIn FiltOut DistIn DistOut RouteMapIn RouteMapOut
Weight
10.10.10.1              unicast
```

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

show route-map

Overview Use this command to display information about one or all route maps.

Syntax

```
show route-map <map-name>
```

Parameter	Description
<map-name>	A name to identify the route map.

Mode User Exec and Privileged Exec

Example To display information about the route-map named `example-map`, use the command:

```
awplus# show route-map example-map
```

Output Figure 30-18: Example output from the **show route-map** command

```
route-map example-map, permit, sequence 1
  Match clauses:
    ip address prefix-list example-pref
  Set clauses:
    metric 100
route-map example-map, permit, sequence 200
  Match clauses:
  Set clauses:
```

Related commands route-map

synchronization

Overview Use this command in Router Configuration mode or in Address Family Configuration mode to ensure BGP does not advertise router learned from iBGP peers until they are learned locally, or are propagated throughout the AS via an IGP.

Use the **no** variant of this command to disable this function.

Syntax

```
synchronization
no synchronization
```

Default Disabled.

Mode Router Configuration and Address Family Configuration mode

Usage notes Synchronization is used when a BGP router should not advertise routes learned from iBGP neighbors, unless those routes are also present in an IGP (for example, OSPF). These routes must be in the RIB (Routing Information Base) learned locally or via an IGP.

Synchronization may be enabled when all the routers in an autonomous system do not speak BGP, and the autonomous system is a transit for other autonomous systems.

Use the **no synchronization** command when BGP router can advertise routes learned from iBGP neighbors, without waiting for IGP reachability, when routes are in the RIB.

Example The following example enables IGP synchronization of iBGP routes in Router Configuration mode:

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# synchronization
```

The following example enables IGP synchronization of iBGP routes in IPv4 unicast Address Family Configuration mode:

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config)# address-family ipv4 unicast
awplus(config-af)# synchronization
```

The following example enables IGP synchronization of iBGP routes in the IPv6 unicast Address Family Configuration mode:

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config)# address-family ipv6 unicast
awplus(config-af)# synchronization
```

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

timers (BGP)

Overview Use this command sets the BGP keepalive timer and holdtime timer values.

Use the **no** variant of this command to reset timers to the default.

Syntax

```
timers bgp <keepalive> <holdtime>
no timers bgp [<keepalive> <holdtime>]
```

Parameter	Description
<keepalive>	*<0-65535>* The frequency with which the keepalive messages are sent to the neighbors. The default is 30 seconds as per RFC 4271. Cisco IOS uses a 60 second keepalive timer default value. Adjust keepalive timers for interoperability as required. Maintain the keepalive value at the holdtime value / 3.
<holdtime>	*<0-65535>* The interval after which the neighbor is considered dead if keepalive messages are not received. The default holdtime value is 90 seconds as per RFC 4271. Cisco IOS uses a 180 second holdtime timer default value. Adjust holdtime timers for interoperability as required. Maintain the holdtime value at the keepalive value * 3.

Default The keepalive timer default is 60 seconds, the holdtime timer default is 90 seconds, and the connect timer default is 120 seconds as per RFC 4271. Holdtime is keepalive * 3.

Mode Router Configuration

Usage notes This command is used globally to set or unset the keepalive and holdtime values for all the neighbors.

Examples

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# timers bgp 40 120
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no timers bgp 30 90
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no timers bgp
```

Related commands

neighbor timers

show ip bgp neighbors hold-time (BGP only)

show ip bgp neighbors keepalive-interval (BGP only)

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

undebug bgp (BGP only)

Overview Use this command to disable BGP debugging functions.

Syntax

```
undebug bgp
[all|dampening|events|filters|fsm|keepalives|nht|nsm|updates]
undebug all bgp
```

Parameter	Description
`all`	Disable all debugging for BGP.
`dampening`	Disable debugging for BGP dampening.
`events`	Disable debugging for BGP events.
`filters`	Disable debugging for BGP filters.
`fsm`	Disable debugging for BGP Finite State Machine (FSM).
`keepalives`	Disable debugging for BGP keepalives.
`nht`	Disable debugging for BGP NHT (Next Hop Tracking) messages.
`nsm`	Disable debugging for NSM messages.
`updates`	Disable debugging for BGP updates.

Mode Privileged Exec and Global Configuration

Example

```
awplus# undebug bgp events
awplus# undebug bgp nht
awplus# undebug bgp updates
```

Related commands debug bgp (BGP only)

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

31 Route Map Commands

Introduction

Overview This chapter provides an alphabetical reference for route map commands. For more information, see the Routemaps Feature Overview and Configuration Guide. These commands can be divided into the following categories:

- the route-map command, which is used to create a route map and/or route map entry, and to put you into route map mode
- **match** commands, used to determine which routes or BGP update messages the route map applies to
- **set** commands, used to modify matching routes or BGP update messages

Command List

- "match as-path" on page 1575
- "match community" on page 1577
- "match interface" on page 1579
- "match ip address" on page 1580
- "match ip next-hop" on page 1582
- "match ipv6 address" on page 1584
- "match ipv6 next-hop" on page 1586
- "match metric" on page 1587
- "match origin" on page 1588
- "match route-type" on page 1590
- "match tag" on page 1591
- "route-map" on page 1592
- "set aggregator" on page 1595
- "set as-path" on page 1596
- "set atomic-aggregate" on page 1597

- "set comm-list delete" on page 1598
- "set community" on page 1599
- "set dampening" on page 1601
- "set extcommunity" on page 1603
- "set ip next-hop (route map)" on page 1605
- "set ipv6 next-hop" on page 1606
- "set local-preference" on page 1607
- "set metric" on page 1608
- "set metric-type" on page 1610
- "set origin" on page 1611
- "set originator-id" on page 1612
- "set tag" on page 1613
- "set weight" on page 1614
- "show route-map" on page 1615

match as-path

Overview Use this command to add an autonomous system (AS) path match clause to a route map entry. Specify the AS path attribute value or values to match by specifying the name of an AS path access list. To create the AS path access list, enter Global Configuration mode and use the ip as-path access-list command.

A BGP update message matches the route map if its attributes include AS path values that match the AS path access list.

Each entry of a route map can only match against one AS path access list in one AS path match clause. If the route map entry already has an AS path match clause, entering this command replaces that match clause with the new clause.

Note that AS path access lists and route map entries both specify an action of deny or permit. The action in the AS path access list determines whether the route map checks update messages for a given AS path value. The route map action and its **set** clauses determine what the route map does with update messages that contain that AS path value.

Use the **no** variant of this command to remove the AS path match clause from a route map entry.

Syntax

```
match as-path <as-path-listname>
no match as-path [<as-path-listname>]
```

Parameter	Description
<as-path-listname>	Specifies an AS path access list name.

Mode Route-map Configuration

Usage notes This command is valid for BGP update messages only.

Example To add entry `34` to the route map called `myroute`, which will discard update messages if they contain the AS path values that are included in `myaccesslist`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute deny 34
awplus(config-route-map)# match as-path myaccesslist
```

Related commands route-map

set as-path

show route-map

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

match community

Overview Use this command to add a community match clause to a route map entry. Specify the community value or values to match by specifying a community list. To create the community list, enter Global Configuration mode and use the ip community-list command.

A BGP update message matches the route map if its attributes include community values that match the community list.

Each entry of a route map can only match against one community list in one community match clause. If the route map entry already has a community match clause, entering this command replaces that match clause with the new clause.

Note that community lists and route map entries both specify an action of deny or permit. The action in the community list determines whether the route map checks update messages for a given community value. The route map action and its **set** clauses determine what the route map does with update messages that contain that community value.

Use the **no** variant of this command to remove the community match clause from a route map.

Syntax

```
match community
{<community-listname>|<1-99>|<100-199>}[exact-match]

no match community
[<community-listname>|<1-99>|<100-199>|exact-match]
```

Parameter	Description
<community-listname>	The community list name or number.
<1-99>	Community list number (standard range).
<100-199>	Community list number (expanded range).
exact-match	Exact matching of communities.

Mode Route-map Configuration

Usage notes This command is valid for BGP update messages only.

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes.

Example To add entry `3` to the route map called `myroute`, which will process update messages if they contain the community values that are included in `mylist`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# match community mylist
```

Related commands

ip community-list

route-map

set comm-list delete

set community

show route-map

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

match interface

Overview Use this command to add an interface match clause to a route map entry. Specify the interface name to match.

A route matches the route map if its interface matches the interface name.

Each entry of a route map can only match against one interface in one interface match clause. If the route map entry already has an interface match clause, entering this command replaces that match clause with the new clause.

Use the **no** variant of this command to remove the interface match clause from the route map entry. Use the **no** variant of this command without a specified interface to remove all interfaces.

Syntax

```
match interface <interface>
no match interface [<interface>]
```

Parameter	Description
<interface>	The VLAN to match, e.g. `vlan2`.

Mode Route-map Configuration

Usage This command is valid for RIP and OSPF routes only.

Example To add entry `10` to the route map called `mymap1`, which will process routes if they use the interface `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map mymap1 permit 10
awplus(config-route-map)# match interface vlan1
```

To remove all interfaces from the route map called `mymap1`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map mymap1 permit 10
awplus(config-route-map)# no match interface
```

Related commands

match ip address

match ip next-hop

match route-type

match tag

route-map

show route-map

match ip address

Overview Use this command to add an IP address prefix match clause to a route map entry. You can specify the prefix or prefixes to match by either:

- specifying the name of an access list. To create the access list, enter Global Configuration mode and use the **access-list** command.
- specifying the name of a prefix list. To create the prefix list, enter Global Configuration mode and use the **ip prefix-list** command.

A route matches the route map entry if the route's prefix matches the access list or prefix list.

Use the **no** variant of this command to remove the IP address match clause from a route map entry. To remove a prefix list-based match clause you must also specify the **prefix-list** parameter.

Syntax

```
match ip address <access-list-id>
match ip address prefix-list <prefix-listname>
no match ip address
no match ip address <access-list-id>
no match ip address prefix-list <prefix-listname>
```

Parameter	Description	
<access-list-id>	Use an ACL to specify which prefixes to match.	
	<access-list-name>	The IP access list name.
	<1-199>	The IP access list number.
	<1300-2699>	The IP access list number (expanded range).
prefix-list	Use an IP prefix list to specify which prefixes to match.	
	<prefix-listname>	The prefix list name.

Mode Route-map Configuration

Usage notes Each entry of a route map can have at most one access list-based IP address match clause and one prefix list-based IP address match clause. If the route map entry already has one of these match clauses, entering this command replaces that match clause with the new clause.

Note that access lists, prefix lists and route map entries all specify an action of deny or permit. The action in the access list or prefix list determines whether the route map checks update messages and routes for a given prefix. The action in the route map, and the map's **set** clauses, determine what the device does with update messages or routes that contain that prefix.

If the **match ip address** command results in a match against the specified IP address, then the outcome is:

- If **permit** is specified, then the route is redistributed or controlled, as specified by the set action.
- If **deny** is specified, then the route is not redistributed or controlled.

If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of **permit** or **deny** specifications.

This command is valid for:

- OSPF routes
- routes in BGP update messages
- RIP routes.

Examples To add entry 3 to the route map called 'myroute', which will process routes that match the ACL called 'List1', use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# match ip address List1
```

To add entry 3 to the route map called 'rmap1', which will process routes that match the prefix list called 'mylist', use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# match ip address prefix-list mylist
```

Related commands

access-list (extended numbered)

access-list (standard numbered)

ip prefix-list

route-map

show ip access-list

show route-map

match ip next-hop

Overview Use this command to add a next-hop match clause to a route map entry. You can specify the next hop to match by either:

- specifying the name of an access list. To create the access list, enter Global Configuration mode and use the **access-list** command.
- specifying the name of a prefix list. To create the prefix list, enter Global Configuration mode and use the **ip prefix-list** command.

A route matches the route map if the route's next hop matches the access list or prefix list.

Each entry of a route map can have at most one access list-based next-hop match clause and one prefix list-based next-hop match clause. If the route map entry already has one of these match clauses, entering this command replaces that match clause with the new clause.

Note that the lists and route map entries specify an action of deny or permit. The action in the list determines whether the route map checks update messages and routes for a given next-hop value. The route map action and its **set** clauses determine what the route map does with update messages and routes that contain that next hop.

Use the **no** variant of this command to remove the next-hop match clause from a route map entry. To remove a prefix list-based match clause you must also specify the prefix-list parameter.

Syntax

```
match ip next-hop <access-list-id>
match ip next-hop prefix-list <prefix-listname>
no match ip next-hop [<access-list-id>]
no match ip next-hop prefix-list [<prefix-listname>]
```

Parameter	Description	
<access-list-id>	Use an ACL to specify which next hops to match.	
	<access-list-name>	The IP access list name.
	<1-199>	The IP access list number.
	<1300-2699>	The IP access list number (expanded range).
prefix-list	Use an IP prefix list to specify which next hops to match.	
	<prefix-listname>	The prefix list name.

Mode Route-map Configuration

Usage notes This command is valid for:

- OSPF routes

- routes in BGP update messages
- RIP routes.

Examples

To add entry 3 to the route map called 'rmap1', which will process routes whose next hop matches the ACL called 'mylist', use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# match ip next-hop mylist
```

To add entry 3 to the route map called 'mymap', which will process routes whose next hop matches the prefix list called 'list1', use the commands:

```
awplus# configure terminal
awplus(config)# route-map mymap permit 3
awplus(config-route-map)# match ip next-hop prefix-list list1
```

Related commands

access-list (extended numbered)

access-list (standard numbered)

ip prefix-list

route-map

show ip access-list

show ip prefix-list

show route-map

match ipv6 address

Overview Use this command to add an IPv6 address prefix match clause to a route map entry. You can specify the prefix or prefixes to match by either:

- specifying the name of an access list. To create the access list, enter Global Configuration mode and use the **access-list** command.
- specifying the name of a prefix list. To create the prefix list, enter Global Configuration mode and use the **ipv6 prefix-list** command.

A route matches the route map entry if the route's prefix matches the access list or prefix list.

Use the **no** variant of this command to remove the IPv6 address match clause from a route map entry.

Syntax

```
match ipv6 address <access-list-id>
match ipv6 address prefix-list <prefix-listname>
no match ipv6 address
no match ipv6 address <access-list-id>
no match ipv6 address prefix-list <prefix-listname>
```

Parameter	Description
<access-list-id>	{<access-list-name>|<1-199>|<1300-2699>} The IP access list name or number.
<access-list-name>	The IP access list name.
<1-199>	The IP access list number.
<1300-2699>	The IP access list number (expanded range).
prefix-list	Use an IP prefix list to specify which prefixes to match.
<prefix-listname>	The prefix list name.

Mode Route-map Configuration

Usage notes Each entry of a route map can have at most one access list-based IPv6 address match clause and one prefix list-based IPv6 address match clause. If the route map entry already has one of these match clauses, entering this command replaces that match clause with the new clause.

Note that access lists, prefix lists and route map entries all specify an action of deny or permit. The action in the access list or prefix list determines whether the route map checks update messages and routes for a given prefix. The action in the route map, and the map's **set** clauses, determine what the device does with update messages or routes that contain that prefix.

If the **match ipv6 address** command results in a match against the specified IPv6 address, then the outcome is:

- If **permit** is specified, then the route is redistributed or controlled, as specified by the set action.
- If **deny** is specified, then the route is not redistributed or controlled.

If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of **permit** or **deny** specifications.

This command is valid for:

- OSPF routes
- routes in BGP update messages
- RIP routes.

Examples To avoid processing the routes specified by the ACL named “acl1”, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 deny 1
awplus(config-route-map)# match ipv6 address acl1
```

To match traffic according to the prefix list named “mylist”, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# match ipv6 address prefix-list mylist
```

match ipv6 next-hop

Overview Use this command to specify a next-hop address to be matched by the route-map.

Use the **no** variant of this command to disable this function.

Syntax

```
match ipv6 next-hop <access-list-name>
match ipv6 next-hop <ipv6-addr>
match ipv6 next-hop prefix-list <prefix-listname>
no match ipv6 next-hop [<access-list-name>]
match ipv6 next-hop [<ipv6-addr>]
match ipv6 next-hop [prefix-list <prefix-listname>]
```

Parameter	Description
<access-list-name>	The name of the IPv6 access list that specifies criteria for the addresses to match.
<ipv6-addr>	The IPv6 address of the next hop. The IPv6 address uses the format X:X::X:X.
<prefix-listname>	The name of the IPv6 prefix list that specifies criteria for the addresses to be matched.

Mode Route-map Configuration

Usage notes The **match ipv6 next-hop** command specifies the next-hop address to be matched. If there is a match for the specified next-hop address, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

NOTE: *This command is valid only for BGP.*

Example

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# match ipv6 next-hop 2001:0db8::/32
```

match metric

Overview Use this command to add a metric match clause to a route map entry. Specify the metric value to match.

A route matches the route map if its metric matches the route map's metric.

A BGP update message matches the route map if its MED attribute value matches the route map's metric.

Each entry of a route map can only match against one metric value in one metric match clause. If the route map entry already has a metric match clause, entering this command replaces that match clause with the new clause.

Use the **no** variant of this command to remove the metric match clause from the route map entry.

Syntax

```
match metric <metric>
no match metric [<metric>]
```

Parameter	Description
<metric>	*<0-4294967295>* Specifies the metric value.

Mode Route-map Configuration

Usage notes This command is valid for:

- OSPF routes
- routes in BGP update messages
- RIP routes.

Example To stop entry 3 of the route map called "myroute" from processing routes with a metric of 888999, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# no match metric 888999
```

Related commands

route-map

set metric

show route-map

match origin

Overview Use this command to add an origin match clause to a route map entry. Specify the origin attribute value to match.

A BGP update message matches the route map if its origin attribute value matches the route map's origin value.

Each entry of a route map can only match against one origin in one origin match clause. If the route map entry already has an origin match clause, entering this command replaces that match clause with the new clause.

Use the **no** variant of this command to remove the origin match clause from the route map entry.

Syntax

```
match origin {egp|igp|incomplete}
no match origin [egp|igp|incomplete]
```

Parameter	Description
`egp`	Learned from an exterior gateway protocol.
`igp`	Learned from a local interior gateway protocol.
`incomplete`	Of unknown heritage, for example a static route.

Mode Route-map Configuration

Usage The origin attribute defines the origin of the path information. The **egp** parameter is indicated as an **e** in the routing table, and it indicates that the origin of the information is learned via Exterior Gateway Protocol. The **igp** parameter is indicated as an **i** in the routing table, and it indicates the origin of the path information is interior to the originating AS. The **incomplete** parameter is indicated as a **?** in the routing table, and indicates that the origin of the path information is unknown or learned through other means. If a static route is redistributed into BGP, the origin of the route is incomplete.

The **match origin** command specifies the origin to be matched. If there is a match for the specified origin, and **permit**is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of **permit** or **deny** specifications.

This command is valid for BGP update messages only.

Example To add entry 34 to the route map called "rmap1", which will drop externally-originated routes, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute deny 34
awplus(config-route-map)# match origin egp
```

Related commands

route-map

set origin

show route-map

match route-type

Overview Use this command to add an external route-type match clause to a route map entry. Specify whether to match OSPF type-1 external routes or OSPF type-2 external routes.

An OSPF route matches the route map if its route type matches the route map's route type.

Each entry of a route map can only match against one route type in one match clause. If the route map entry already has a route type match clause, entering this command replaces that match clause with the new clause.

Use the **no** variant of this command to remove the route type match clause from the route map entry.

Syntax

```
match route-type external {type-1|type-2}
no match route-type external [type-1|type-2]
```

Parameter	Description
`type-1`	OSPF type-1 external routes.
`type-2`	OSPF type-2 external routes.

Mode Route-map Configuration

Usage Use the **match route-type external**command to match specific external route types. AS- external LSA is either Type-1 or Type-2. **external type-1** matches only Type 1 external routes, and **external type-2** matches only Type 2 external routes.

This command is valid for OSPF routes only.

Example To add entry `10` to the route map called `mymap1`, which will process type-1 external routes, use the commands:

```
awplus# configure terminal
awplus(config)# route-map mymap1 permit 10
awplus(config-route-map)# match route-type external type-1
```

Related commands

match interface

match ip address

match ip next-hop

match tag

route-map

set metric-type

show route-map

match tag

Overview Use this command to add a tag match clause to a route map entry. Specify the route tag value to match.

An OSPF route matches the route map if it has been tagged with the route map's tag value. Routes can be tagged through OSPF commands or through another route map's set clause.

Each entry of a route map can only match against one tag in one match clause. If the route map entry already has a tag match clause, entering this command replaces that match clause with the new clause.

Use the **no** variant of this command to remove the tag match clause from the route map entry.

Syntax

```
match tag <0-4294967295>
no match tag [<0-4294967295>]
```

Mode Route-map Configuration

Usage This command is valid for OSPF routes only.

Example To add entry 10 to the route map called `mymap1`, which will process routes that are tagged `100`, use the following commands:

```
awplus# configure terminal
awplus(config)# route-map mymap1 permit 10
awplus(config-route-map)# match tag 100
```

Related commands

match interface

match ip address

match ip next-hop

match route-type

route-map

set tag

show route-map

route-map

Overview Use this command to configure a route map entry, and to specify whether the device will process or discard matching routes and BGP update messages.

The device uses a name to identify the route map, and a sequence number to identify each entry in the route map.

The **route-map** command puts you into route-map configuration mode. In this mode, you can use the following:

- one or more of the **match** commands to create match clauses. These specify what routes or update messages match the entry.
- one or more of the **set** commands to create set clauses. These change the attributes of matching routes or update messages.

Use the **no** variant of this command to delete a route map or to delete an entry from a route map.

Syntax

```
route-map <mapname> {deny|permit} <seq>
no route-map <mapname>
no route-map <mapname> {deny|permit} <seq>
```

Parameter	Description
<mapname>	A name to identify the route map.
`deny`	The route map causes a routing process to discard matching routes or BGP update messages.
`permit`	The route map causes a routing process to use matching routes or BGP update messages.
<seq>	<1-65535> The sequence number of the entry. You can use this parameter to control the order of entries in this route map.

Mode Global Configuration

Usage notes Route maps allow you to control and modify routing information by filtering routes and setting route attributes. You can apply route maps when the device:

- processes BGP update messages that it has received from a peer
- prepares BGP update messages to send to peers
- redistributes routes from one routing protocol into another
- redistributes static routes into routing protocols
- uses BGP route flap dampening

When a routing protocol passes a route or update message through a route map, it checks the entries in order of their sequence numbers, starting with the lowest numbered entry.

If it finds a match on a route map with an action of permit, then it applies any set clauses and accepts the route. Having found a match, the route is not compared against any further entries of the route map.

If it finds a match on a route map with an action of deny, it will discard the matching route.

If it does not find a match, it discards the route or update message. This means that route maps end with an implicit deny entry. To permit all non-matching routes or update messages, end your route map with an entry that has an action of **permit** and no match clause.

Examples

To enter route-map mode for entry 1 of the route map called "route1", and then add a match and set clause to it, use the commands:

```
awplus# configure terminal
awplus(config)# route-map route1 permit 1
awplus(config-route-map)# match as-path 60
awplus(config-route-map)# set weight 70
```

To enter route-map mode for entry 2 of the route map called "route1", and then add a match and set clause to it, use the commands:

```
awplus# configure terminal
awplus(config)# route-map route1 permit 2
awplus(config-route-map)# match interface vlan2
awplus(config-route-map)# set metric 20
```

Note how the prompt changes when you go into route map configuration mode.

To make the device process non-matching routes instead of discarding them, add a command like the following one:

```
awplus(config)# route-map route1 permit 100
```

Related commands

For BGP:

show route-map

bgp dampening

neighbor default-originate

neighbor route-map

neighbor unsuppress-map

network (BGP and BGP4+)

redistribute (into BGP or BGP4+)

show ip bgp route-map (BGP only)

For OSPF:

distribute-list (OSPF)

default-information originate

redistribute (OSPF)

For RIP:

redistribute (RIP)

set aggregator

Overview Use this command to add an aggregator set clause to a route map entry.

When a BGP update message matches the route map entry, the device sets the update's aggregator attribute. The aggregator attribute specifies the AS and IP address of the device that performed the aggregation.

Use the **no** variant of this command to remove the set clause.

Syntax

```
set aggregator as <asnum> <ip-address>
no set aggregator as
```

Parameter	Description
<asnum>	The AS number of the aggregator.
<ip-address>	The IP address of the aggregator.

Mode Route-map Configuration

Usage An Autonomous System (AS) is a collection of networks under a common administration sharing a common routing strategy. It is subdivided by areas, and is assigned a unique 16- bit number. Use the **set aggregator** command to assign an AS number for the aggregator.

This command is valid for BGP update messages only.

Example To use entry `3` of the route map called `myroute` to set the aggregator attribute to `43 10.10.0.3` in matching update messages, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# set aggregator as 43 10.10.0.3
```

To remove all aggregator attributes for entry `3` of the route map called `myroute`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# no set aggregator as
```

Related commands route-map

show route-map

set as-path

Overview Use this command to add an AS path set clause to a route map entry.

When a BGP update message matches the route map entry, the device prepends the specified Autonomous System Number (ASN) or ASNs to the update's AS path attribute.

The AS path attribute is a list of the autonomous systems through which the announcement for the prefix has passed. As prefixes pass between autonomous systems, each autonomous system adds its ASN to the beginning of the list. This means that the AS path attribute can be used to make routing decisions.

Use the **no** variant of this command to remove the set clause.

Syntax

```
set as-path prepend <1-65535> [<1-65535>]...
no set as-path prepend [<1-65535> [<1-65535>]...]
```

Parameter	Description
`prepend`	Prepends the autonomous system path.
<1-65535>	The number to prepend to the AS path. If you specify multiple ASNs, separate them with spaces.

Mode Route-map mode

Usage notes Use the **set as-path** command to specify an autonomous system path. By specifying the length of the AS-Path, the device influences the best path selection by a neighbor. Use the `prepend` parameter with this command to prepend an AS path string to routes increasing the AS path length.

This command is valid for BGP update messages only.

Example To use entry `3` of the route map called `myroute` to prepend ASN `8` and `24` to the AS path of matching update messages, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# set as-path prepend 8 24
```

Related commands

match as-path

route-map

show route-map

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

set atomic-aggregate

Overview Use this command to add an atomic aggregate set clause to a route map entry.

When a BGP update message matches the route map entry, the device adds the atomic aggregate attribute to the update.

Use the **no** variant of this command to remove the set clause.

Syntax
```
set atomic-aggregate
no set atomic-aggregate
```

Mode Route-map Configuration

Usage This command is valid for BGP update messages only.

Example To use entry `3` of the route map called `rmap1` to add the atomic aggregator attribute to matching update messages, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set atomic-aggregate
```

Related commands route-map

show route-map

set comm-list delete

Overview Use this command to delete one or more communities from the community attribute of a BGP update message. Specify the communities to delete by specifying a community list. To create the community list, enter Global Configuration mode and use the ip community-list command.

When a BGP update message matches the route map entry, the device deletes the specified communities from the update's community attribute.

Use the **no** variant of this command to stop deleting the communities.

Syntax

```
set comm-list {<1-199>|<100-199>|<word>} delete
no set comm-list {<1-199>|<100-199>|<word>} delete
```

Parameter	Description
<1-99>	Standard community-list number.
<100-199>	Expanded community-list number.
<word>	Name of the Community-list.

Mode Route-map Configuration

Usage This command is valid for BGP update messages only.

Example To use entry `3` of the route map called `myroute` to delete the communities in community list `34` from matching update messages, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# set comm-list 34 delete
```

Related commands

ip community-list

match community

route-map

set community

show route-map

set community

Overview Use this command to add a community set clause to a route map entry.

When a BGP update message matches the route map entry, the device takes one of the following actions:

- changes the update's community attribute to the specified value or values, or
- adds the specified community value or values to the update's community attribute, if you specify the **additive** parameter after specifying another parameter. or
- removes the community attribute from the update, if you specify the **none** parameter

Use the **no** variant of this command to remove the set clause.

Syntax

```
set community {[<1-65535>][AA:NN] [internet] [local-AS]
[no-advertise] [no-export] [additive]}
```

```
no set community {[AA:NN] [internet] [local-AS] [no-advertise]
[no-export] [additive]}
```

```
set community none
```

```
no set community none
```

Parameter	Description
<1-65535>	The AS number of the community as an integer not in AA:NN format.
AA:NN	The Autonomous System (AS) number of the community, in AA:NN format. AS numbers are assigned to the regional registries by the IANA (www.iana.org) and can be obtained from the registry in your region. AA and NN are both integers from 1 to 65535. AA is the AS number; NN is a value chosen by the ASN administrator.
`local-AS`	The community of routes that must not be advertised to external BGP peers (this includes peers in other members' Autonomous Systems inside a BGP confederation).
`internet`	The community of routes that can be advertised to all BGP peers.
`no-advertise`	The community of routes that must not be advertised to other BGP peers.
`no-export`	The community of routes that must not be advertised outside a BGP confederation boundary (a standalone Autonomous System that is not part of a confederation should be considered a confederation itself).

Parameter	Description
`none`	The device removes the community attribute from matching update messages.
`additive`	The device adds the specified community value to the update message's community attribute, instead of replacing the existing attribute. By default this parameter is not included, so the device replaces the existing attribute.

Mode Route-map Configuration

Usage notes This command is valid for BGP update messages only.

Examples To use entry `3` of the route map called `rmap1` to put matching routes into the no-advertise community, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community no-advertise
```

To use entry `3` of the route map called `rmap1` to put matching routes into several communities, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community 10:01 23:34 12:14
no-export
```

To use entry `3` of the route map called `rmap1` to put matching routes into a single AS community numbered `16384`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community 16384 no-export
```

Related commands

match community

route-map

set aggregator

set comm-list delete

set extcommunity

show route-map

Command changes Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for IEx510, x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

set dampening

Overview Use this command to add a route flap dampening set clause to a route map entry.

Also use the route map by specifying it in the command bgp dampening route-map.

When a route matches the route map entry, the device enables route flap dampening for that route. If the set clause includes dampening parameter values, the device uses those values when dampening the matching route.

Use the **no** variant of this command to remove the set clause. This disables dampening on matching routes.

Syntax

```
set dampening
set dampening [<reachtime>]
set dampening <reachtime> [<reuse> <suppress> <maxsuppress>] [<unreachtime>]
no set dampening
no set dampening [<reachtime>]
no set dampening <reachtime> [<reuse> <suppress> <maxsuppress>] [<unreachtime>]
```

Parameter	Description
<reachtime>	*<1-45>* The time it takes, in minutes, for the route's instability penalty to halve if the route remains stable. The instability penalty is called the Figure of Merit (FoM). For example, if reachtime is 15, the FoM of a stable route halves over a 15 minute period, quarters over a 30 minute period, and so on. The default is 15 minutes.
<reuse>	*<1-20000>* The value that the instability penalty (FoM) must reach for the device to use a suppressed route again. Once a route is suppressed, it remains suppressed until its FoM falls below this threshold. Reuse must not exceed suppress. The default is 750.
<suppress>	*<1-20000>* The instability penalty (FoM) at which the route is suppressed. Suppress must be greater than or equal to reuse. If suppress is less than 1000, a route is suppressed when it becomes unreachable for the first time. The default is 2000.

Parameter	Description
<maxsuppress>	*<1-255>* A number that is multiplied by reachtime to give the maximum time in minutes for which a suppressed route must remain stable in order to become unsuppressed. The lowest maxsuppress value of 1 gives a maximum suppression time of 1 x reachtime, and the highest maxsuppress value of 255 gives a maximum suppression time of 255 x reachtime. For example, if reachtime is 15 and maxsuppress is 4, the route is unsuppressed after 60 minutes of stability even if its FoM still exceeds reuse. The default is 4.
<unreachtime>	*<1-45>* The time it takes, in minutes, for the route's instability penalty to halve if the route remains unstable. The default is 15 minutes.

Mode Route-map Configuration

Usage Set the unreachability half-life time to be equal to, or greater than, reachability half-life time. The suppress-limit value must be greater than or equal to the reuse limit value.

This command is valid for BGP routes only.

Example To use entry 24 of the route map called `R1` to enable dampening of matching routes and set the dampening parameters, use the commands:

Related commands bgp dampening

route-map

show route-map

set extcommunity

Overview Use this command to add an extended community set clause to a route map entry. A route map entry can have a route target extended community set clause, a site-of-origin extended community set clause, or both.

When a BGP update message matches the route map entry, the device sets the update's extended community attribute to the specified value or values.

Use the **no** variant of this command to remove the set clause.

Syntax

```
set extcommunity {rt|soo} <extcomm-number>
no set extcommunity {rt|soo} [<extcomm-number>]
```

Parameter	Description
`rt`	Configure a route target extended community. This consists of routers that will receive matching routes.
`soo`	Configure a site-of-origin extended community. This consists of routers that will inject matching routes into BGP.
<extcomm-number>	The extended community number, in the format AA:NN or IPADD:N.

Mode Route-map Configuration

Usage notes This command is valid for BGP update messages only.

Examples To use entry `3` of the route map called `rmap1` to set the route target extended community attribute to 06:01, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set extcommunity rt 06:01
```

To instead specify the extended community number in dotted decimal notation, use the command:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set extcommunity rt 0.0.0.6:01
```

To use entry `3` of the route map called `rmap1` to set the site-of-origin extended community attribute to 06:01, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set extcommunity soo 06:01
```

To instead specify the extended community number in dotted decimal notation, use the command:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set extcommunity soo 0.0.0.6:01
```

Related commands

match community

route-map

set comm-list delete

set community

show route-map

set ip next-hop (route map)

Overview Use this command to add a next-hop set clause to a route map entry.

When a route or BGP update message matches the route map entry, the device sets the route's next hop to the specified IP address.

Use the **no** variant of this command to remove the set clause.

Syntax

```
set ip next-hop <ip-address>
no set ip next-hop [<ip-address>]
```

Parameter	Description
<ip-address>	The IP address of the next hop, entered in the form A.B.C.D.

Mode Route-map Configuration

Usage notes Use this command to set the next-hop IP address to the routes.

This command is valid for:

- OSPF routes
- routes in BGP update messages
- RIP routes.

Example To use entry 3 of the route map called `mymap` to give matching routes a next hop of 10.10.0.67, use the commands:

```
awplus# configure terminal
awplus(config)# route-map mymap permit 3
awplus(config-route-map)# set ip next-hop 10.10.0.67
```

Related commands

match ip next-hop

route-map

show route-map

set ipv6 next-hop

Overview Use this command to set a next hop-address.

Use the **no** variant of this command to delete an entry.

Syntax

```
set ipv6 next-hop {<ipv6-addr-global>|local <ipv6-addr>}
no set ipv6 next-hop [<ipv6-addr-global>|local [<ipv6-addr>]]
```

Parameter	Description
<ipv6-addr-global>	The IPv6 global address of next hop. The IPv6 address uses the format X:X::X:X.
`local`	Specifies that the address is local.
<ipv6-addr>	The IPv6 local address of next hop. The IPv6 address uses the format X:X::X:X.

Mode Route-map Configuration

Usage notes Use this command to set the next-hop IPv6 address to the routes.

This command is valid only for BGP.

Examples

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set ipv6 next-hop local
fe80::203:47ff:fe97:66dc
awplus(config-route-map)# no set ipv6 next-hop
```

set local-preference

Overview This command changes the default local preference value.

The local preference indicates the BGP local preference path attribute when there are multiple paths to the same destination. The path with the higher preference is chosen.

Use this command to define the preference of a particular path. The preference is sent to all routers and access servers in the local autonomous system.

The **no** variant of this command reverts to the default setting.

Syntax

```
set local-preference <pref-value>
no set local-preference [<pref-value>]
```

Parameter	Description
<pref-value>	<0-4294967295> Configure local preference value. The default local preference value is 100.

Mode Route-map Configuration

Examples

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set local-preference 2345555
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-route-map)# no set local-preference
```

Related commands For related Route Map commands:

route-map

show route-map

For related BGP commands:

bgp default local-preference (BGP only)

neighbor route-map

set metric

Overview Use this command to add a metric set clause to a route map entry.

When a route or BGP update message matches the route map entry, the device takes one of the following actions:

- changes the metric (or for BGP, the MED attribute value) to the specified value, or
- adds or subtracts the specified value from the metric or MED attribute, if you specify + or - before the value (for example, to increase the metric by 2, enter +2)

Use the **no** variant of this command to remove the set clause.

Syntax

```
set metric {+<metric-value>|-<metric-value>|<metric-value>}
no set metric [+<metric-value>|-<metric-value>|<metric-value>]
```

Parameter	Description
+	Increase the metric or MED attribute by the specified amount.
–	Decrease the metric or MED attribute by the specified amount.
<metric-value>	<0-4294967295> The new metric or MED attribute value, or the amount by which to increase or decrease the existing value.

Default The default metric value for routes redistributed into OSPF and OSPFv3 is 20.

Mode Route-map Configuration

Usage notes For BGP, if you want the device to compare MED values in update messages from peers in different ASes, also enter the command bgp always-compare-med. You do not need to enter this command if you only want the device to compare MED values in update messages from peers in the same AS, because it always does.

This command is valid for:

- OSPF routes
- routes in BGP update messages
- RIP routes.

Note that defining the OSPF metric in a route map supersedes the metric defined using a redistribute (OSPF) or a redistribute (IPv6 OSPF) command. For more information, see the OSPFv3 Feature Overview and Configuration Guide and the OSPF Feature Overview and Configuration Guide.

Examples

To use entry 3 of the route map called "rmap1" to give matching routes a metric of 600, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set metric 600
```

To use entry 3 of the route map called "rmap1" to increase the metric of matching routes by 2, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set metric +2
```

Related commands

match metric

route-map

show route-map

set metric-type

Overview Use this command to add a metric-type set clause to a route map entry.

When a route matches the route map entry, the device sets its route type to the specified value.

Use the **no** variant of this command to remove the set clause.

Syntax

```
set metric-type {type-1|type-2}
no set metric-type [type-1|type-2]
```

Parameter	Description
`type-1`	Redistribute matching routes into OSPF as type-1 external routes.
`type-2`	Redistribute matching routes into OSPF as type-2 external routes.

Mode Route-map Configuration

Usage notes This command is valid for OSPF routes only.

Example To use entry `3` of the route map called `rmap1` to redistribute matching routes into OSPF as type-1 external routes, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set metric-type 1
```

Related commands

default-information originate

redistribute (OSPF)

match route-type

route-map

show route-map

set origin

Overview Use this command to add an origin set clause to a route map entry.

When a BGP update message matches the route map entry, the device sets its origin attribute to the specified value.

Use the **no** variant of this command to remove the set clause.

Syntax

```
set origin {egp|igp|incomplete}
no set origin [egp|igp|incomplete]
```

Parameter	Description
`egp`	Learned from an exterior gateway protocol.
`igp`	Learned from a local interior gateway protocol.
`incomplete`	Of unknown heritage, for example a static route.

Mode Route-map Configuration

Usage This command is valid for BGP update messages only.

Example To use entry `3` of the route map called `rmap1` to give matching update messages an origin of `egp`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set origin egp
```

Related commands

match origin

route-map

show route-map

set originator-id

Overview Use this command to add an originator ID set clause to a route map entry.

The originator ID is the router ID of the IBGP peer that first learned this route, either via an EBGP peer or by some other means such as importing it.

When a BGP update message matches the route map entry, the device sets its originator ID attribute to the specified value.

Use the **no** variant of this command to remove the set clause.

Syntax

```
set originator-id <ip-address>
no set originator-id [<ip-address>]
```

Parameter	Description
<ip-address>	The IP address of the originator, entered in the form A.B.C.D.

Mode Route-map Configuration

Usage This command is valid for BGP update messages only.

Example To use entry `3` of the route map called `rmap1` to give matching update messages an originator ID of `1.1.1.1`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set originator-id 1.1.1.1
```

Related commands route-map

show route-map

set tag

Overview Use this command to add a tag set clause to a route map entry.

When a route matches the route map entry, the device sets its tag to the specified value when it redistributes the route into OSPF.

Use the **no** variant of this command to remove the set clause.

Syntax

```
set tag <tag-value>
no set tag [<tag-value>]
```

Parameter	Description
<tag-value>	<0-4294967295> Value to tag matching routes with.

Mode Route-map Configuration

Usage notes This command is valid only when redistributing routes into OSPF.

Example To use entry 3 of the route map called `rmap1` to tag matching routes with the number 6, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set tag 6
```

Related commands

default-information originate

redistribute (OSPF)

match tag

route-map

show route-map

set weight

Overview Use this command to add a weight set clause to a route map entry.

The weight value assists in best path selection of BGP routes. It is stored with the route in the BGP routing table, but is not advertised to peers. When there are multiple routes with a common destination, the device uses the route with the highest weight value.

When a route matches the route map entry, the device sets its weight to the specified value.

Use the **no** variant of this command to remove the set clause.

Syntax

```
set weight <weight>
no set weight [<weight>]
```

Parameter	Description
<weight>	*<0-4294967295>* The weight value.

Mode Route-map Configuration

Usage This command is valid for BGP routes only.

Example To use entry `3` of the route map called `rmap1` to give matching routes a weight of `60`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set weight 60
```

Related commands route-map

show route-map

show route-map

Overview Use this command to display information about one or all route maps.

Syntax

```
show route-map <map-name>
```

Parameter	Description
<map-name>	A name to identify the route map.

Mode User Exec and Privileged Exec

Example To display information about the route-map named `example-map`, use the command:

```
awplus# show route-map example-map
```

Output Figure 31-1: Example output from the **show route-map** command

```
route-map example-map, permit, sequence 1
  Match clauses:
    ip address prefix-list example-pref
  Set clauses:
    metric 100
route-map example-map, permit, sequence 200
  Match clauses:
  Set clauses:
```

Related commands route-map

Part 4: Multicast Applications

32 IGMP and IGMP Snooping Commands

Introduction

Overview

Devices running AlliedWare Plus use IGMP (Internet Group Management Protocol) and MLD (Multicast Listener Discovery) to track which multicast groups their clients belong to. This enables them to send the correct multimedia streams to the correct destinations. IGMP is used for IPv4 multicasting, and MLD is used for IPv6 multicasting.

This chapter describes the commands to configure IGMP Querier behaviour and selection, IGMP Snooping and IGMP Proxy.

Command List

- "clear ip igmp" on page 1619
- "clear ip igmp group" on page 1620
- "clear ip igmp interface" on page 1621
- "debug igmp" on page 1622
- "ip igmp" on page 1623
- "ip igmp access-group" on page 1624
- "ip igmp flood-group" on page 1625
- "ip igmp flood specific-query" on page 1627
- "ip igmp immediate-leave" on page 1628
- "ip igmp last-member-query-count" on page 1629
- "ip igmp last-member-query-interval" on page 1630
- "ip igmp limit" on page 1631
- "ip igmp maximum-groups" on page 1632
- "ip igmp mroute-proxy" on page 1634
- "ip igmp proxy-service" on page 1635
- "ip igmp querier-timeout" on page 1636

- "ip igmp query-holdtime" on page 1637
- "ip igmp query-interval" on page 1639
- "ip igmp query-max-response-time" on page 1641
- "ip igmp ra-option" on page 1643
- "ip igmp robustness-variable" on page 1644
- "ip igmp snooping" on page 1645
- "ip igmp snooping fast-leave" on page 1646
- "ip igmp snooping mrouter" on page 1647
- "ip igmp snooping querier" on page 1648
- "ip igmp snooping report-suppression" on page 1649
- "ip igmp snooping routermode" on page 1650
- "ip igmp snooping source-timeout" on page 1652
- "ip igmp snooping tcn query solicit" on page 1653
- "ip igmp source-address-check" on page 1655
- "ip igmp ssm" on page 1656
- "ip igmp ssm-map enable" on page 1657
- "ip igmp ssm-map static" on page 1658
- "ip igmp static-group" on page 1660
- "ip igmp startup-query-count" on page 1662
- "ip igmp startup-query-interval" on page 1663
- "ip igmp trusted" on page 1664
- "ip igmp version" on page 1665
- "show debugging igmp" on page 1666
- "show ip igmp groups" on page 1667
- "show ip igmp interface" on page 1669
- "show ip igmp proxy" on page 1671
- "show ip igmp proxy groups" on page 1672
- "show ip igmp snooping mrouter" on page 1674
- "show ip igmp snooping routermode" on page 1675
- "show ip igmp snooping source-timeout" on page 1676
- "show ip igmp snooping statistics" on page 1677
- "undebug igmp" on page 1679

clear ip igmp

Overview Use this command to clear all IGMP group membership records on all VLAN interfaces.

Syntax
```
clear ip igmp
```

Mode Privileged Exec

Example
```
awplus# clear ip igmp
```

Related commands
clear ip igmp group

clear ip igmp interface

show ip igmp interface

show running-config

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

clear ip igmp group

Overview Use this command to clear IGMP group membership records for a specific group on either all interfaces, a single interface, or for a range of interfaces.

Syntax

```
clear ip igmp group *
clear ip igmp group <ip-address> <interface>
```

Parameter	Description
*	Clears all groups on all interfaces. This has the same effect as the **clear ip igmp** command.
<ip-address>	Specifies the group whose membership records will be cleared from all interfaces, entered in the form A.B.C.D.
<interface>	Specifies the name of the interface; all groups learned on this interface are deleted.

Mode Privileged Exec

Usage notes This command applies to groups learned by IGMP, IGMP Snooping, or IGMP Proxy.

In addition to the group, an interface can be specified. Specifying this will mean that only entries with the group learned on the interface will be deleted.

Examples To delete all group records, use the command:

```
awplus# clear ip igmp group *
```

To delete records for 224.1.1.1 on vlan1, use the command:

```
awplus# clear ip igmp group 224.1.1.1 vlan1
```

Related commands

clear ip igmp

clear ip igmp interface

show ip igmp interface

show running-config

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

clear ip igmp interface

Overview Use this command to clear IGMP group membership records on a particular interface.

Syntax

```
clear ip igmp interface <interface>
```

Parameter	Description
<interface>	Specifies the name of the interface. All groups learned on this interface are deleted.

Mode Privileged Exec

Usage notes This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example To delete records for vlan1, use the command:

```
awplus# clear ip igmp interface vlan1
```

Related commands

clear ip igmp

clear ip igmp group

show ip igmp interface

show running-config

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

debug igmp

Overview Use this command to enable debugging of either all IGMP or a specific component of IGMP.

Use the **no** variant of this command to disable all IGMP debugging, or debugging of a specific component of IGMP.

Syntax

```
debug igmp {all|decode|encode|events|fsm|tib}
no debug igmp {all|decode|encode|events|fsm|tib}
```

Parameter	Description
`all`	Enable or disable all debug options for IGMP
`decode`	Debug of IGMP packets that have been received
`encode`	Debug of IGMP packets that have been sent
`events`	Debug IGMP events
`fsm`	Debug IGMP Finite State Machine (FSM)
`tib`	Debug IGMP Tree Information Base (TIB)

Modes Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# debug igmp all
```

Related commands show debugging igmp

undebug igmp

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip igmp

Overview Use this command to enable IGMP on an interface. The command configures the device as an IGMP querier.

Use the **no** variant of this command to return all IGMP related configuration to the default on this interface.

Syntax

```
ip igmp
no ip igmp
```

Default Disabled

Mode Interface Configuration for a VLAN interface.

Usage notes An IP address must be assigned to the interface first, before this command will work.

Example To specify an interface as an IGMP querier, use the commands:

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

Validation Commands show ip igmp interface

show running-config

ip igmp access-group

Overview This command adds an access control list to a VLAN interface configured for IGMP, IGMP Snooping, or IGMP Proxy. The access control list is used to control and filter the multicast groups learned on the VLAN interface.

The **no** variant of this command disables the access control filtering on the interface.

Syntax

```
ip igmp access-group {<access-list-number>|<access-list-name>}
no ip igmp access-group
```

Parameter	Description
<access-list-number>	Standard IP access-list number, in the range <1-99>.
<access-list-name>	Standard IP access-list name.

Default By default there are no access lists configured on any interface.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to VLAN interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example In the following example, hosts serviced by VLAN interface vlan2 can only join the group `225.2.2.2`:

```
awplus# configure terminal
awplus(config)# access-list 1 permit 225.2.2.2 0.0.0.0
awplus(config)# interface vlan2
awplus(config-if)# ip igmp access-group 1
```

ip igmp flood-group

Overview Use this command to configure a static multicast group that will flood matching packets to all ports in the VLAN and not mirror any packets matching that group to the CPU.

Use the **no** variant of this command to remove an IGMP flooding group.

Syntax

```
ip igmp flood-group <ip-address> [<vlan-id>]
no ip igmp flood-group <ip-address>
```

Parameter	Description
<ip-address>	Standard IP Multicast group address, entered in the form A.B.C.D.
<vlan-id>	Layer 3 downstream interface list for Layer 3 forwarding of multicast packets.

Default Not set.

Mode Interface Configuration

Usage notes Multicast packets from an unregistered source will be mirrored to the CPU to ensure IGMP and PIM-SM knows about the group. In certain networks, it is possible for a large number of packets with a number of different sources destined for the same group address, to overwhelm a switches hardware table. This could cause packets to be stuck mirrored to the CPU forever, resulting in high CPU usage and in some cases stack failovers.

This command adds an all sources multicast entry into the switches multicast hardware table, to flood multicast packets to all ports within the VLAN without mirroring the traffic to CPU. This significantly reduces the number of hardware entries consumed.

The Layer 3 variant of this command:

```
ip igmp flood-group <ip-address> <vlan-id>
```

is only supported on one VLAN group address. Any number of the Layer 2 variants can be used.

Example To configure an IGMP flooding group to Layer 2 ports only, use the following commands. This will flood any UDP packet to group 239.255.255.250 to all ports in vlan1:

```
awplus# configure terminal
awplus(config)# int vlan1
awplus(config-if)# ip igmp flood-group 239.255.255.250
```

To configure an IGMP flooding group to Layer 2 ports and Layer 3 forwarding, use the following commands. This will flood any UDP packet to group 239.255.255.250 to all ports in vlan2 and forward any UDP packet to all ports in vlan3:

```
awplus# configure terminal
awplus(config)# int vlan2
awplus(config-if)# ip igmp flood-group 239.255.255.250 vlan3
```

To remove an IGMP flooding group from vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# int vlan2
awplus(config-if)# no ip igmp flood-group 239.255.255.250
```

IGMP Flooding Groups are integrated into the existing command: **show ip igmp groups**

Output Figure 32-1: Example output from **show ip igmp groups**

```
awplus#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface   Uptime    Expires  Last Reporter
239.255.255.250  vlan3000    01:20:59  stopped 0.0.0.0
```

Related commands ip igmp static-group

Command changes Version 5.5.0-2.3: command added

ip igmp flood specific-query

Overview Use this command if you want IGMP to flood specific queries to all VLAN member ports, instead of only sending the queries to multicast group member ports.

Use the **no** variant of this command if you want IGMP to only send the queries to multicast group member ports.

Syntax

```
ip igmp flood specific-query
no ip igmp flood specific-query
```

Default By default, specific queries are flooded to all VLAN member ports.

Mode Global Configuration

Usage In an L2 switched network running IGMP, it is considered more robust to flood all specific queries. In most cases, the benefit of flooding specific queries to all VLAN member ports outweighs the disadvantages.

However, sometimes this is not the case. For example, if hosts with very low CPU capability receive specific queries for multicast groups they are not members of, their performance may degrade unacceptably. In this situation, it is desirable for IGMP to send specific queries to known member ports only. This minimizes the performance degradation of such hosts. In those circumstances, use this command to turn off flooding of specific queries.

Example To cause IGMP to flood specific queries only to multicast group member ports, use the commands:

```
awplus# configure terminal
awplus(config)# no ip igmp flood specific-query
```

Related commands show ip igmp interface

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip igmp immediate-leave

Overview In IGMP version 2, use this command to minimize the leave latency of IGMP memberships for specified multicast groups. The specified access list number or name defines the multicast groups in which the immediate leave feature is enabled.

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

Syntax

```
ip igmp immediate-leave group-list
{<access-list-number>|<access-list-number-expanded>|
<access-list-name>}
```

```
no ip igmp immediate-leave
```

Parameter	Description
<access-list-number>	Access-list number, in the range <1-99>.
<access-list-number-expanded>	Access-list number (expanded range), in the range <1300-1999>.
<access-list-name>	Standard IP access-list name.

Default Disabled by default.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to VLAN interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example The following example shows how to enable the immediate-leave feature on the VLAN interface vlan2 for a specific range of multicast groups:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp immediate-leave group-list 34
awplus(config-if)# exit
awplus(config)# access-list 34 permit 225.192.20.0 0.0.0.255
```

Related commands ip igmp last-member-query-interval

ip igmp last-member-query-count

Overview Use this command to set the last-member query-count value for an interface.

Use the **no** variant of this command to return to the default on an interface.

Syntax

```
ip igmp last-member-query-count <2-7>
no ip igmp last-member-query-count
```

Parameter	Description
<2-7>	Last member query count value.

Default The default last member query count value is 2.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to VLAN interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example To set the last-member query-count to 3 on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp last-member-query-count 3
```

Related commands

ip igmp last-member-query-interval

ip igmp startup-query-count

show ip igmp interface

show running-config

ip igmp last-member-query-interval

Overview Use this command to configure the frequency at which the router sends IGMP group specific host query messages.

Use the **no** variant of this command to set this frequency to the default.

Syntax

```
ip igmp last-member-query-interval <interval>
no ip igmp last-member-query-interval
```

Parameter	Description
<interval>	The frequency in milliseconds at which IGMP group-specific host query messages are sent, in the range 1000-25500.

Default 1000 milliseconds

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to VLAN interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example To change the IGMP group-specific host query message interval to 2 seconds (2000 milliseconds) on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp last-member-query-interval 2000
```

Related commands

ip igmp immediate-leave

ip igmp last-member-query-count

show ip igmp interface

show running-config

ip igmp limit

Overview Use this command to configure the limit on the maximum number of group membership entries for the device as a whole or for the specified interface (if in interface mode). Once the specified number of group memberships is reached, all further membership reports will be ignored.

Optionally, you can configure an access-list to stop certain addresses from being subject to the limit.

Use the **no** variant of this command to unset the limit and any specified exception access-list.

Syntax

```
ip igmp limit <limit-value> [except
{<access-list-number>|<access-list-number-expanded>|
<access-list-name>}]
```

```
no ip igmp limit
```

Parameter	Description
<limit-value>	Maximum number of group membership entries, from 2 to 512.
<access-list-number>	Access-list number, in the range 1 to 99.
<access-list-number-expanded>	Access-list number (expanded range), in the range 1300 to 1999.
<access-list-name>	IP access-list name.

Default 512

Mode Global Configuration and Interface Configuration for a VLAN interface.

Usage notes This command applies to VLAN interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example To configure an IGMP limit of 100 group membership entries on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp limit 100
```

To configure an IGMP limit of 100 group membership entries across all interfaces on which IGMP is enabled, and exclude group 224.1.1.1 from this limitation, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 1 permit 224.1.1.1 0.0.0.0
awplus(config)# ip igmp limit 100 except 1
```

ip igmp maximum-groups

Overview Use this command to set a limit, per switch port, on the number of IGMP groups clients can join. This stops a single client from using all the switch's available group-entry resources, and ensures that clients on all ports have a chance to join IGMP groups.

Use the **no** variant of this command to remove the limit.

Syntax

```
ip igmp maximum-groups <0-65535>
no ip igmp maximum-groups
```

Parameter	Description
<0-65535>	The maximum number of IGMP groups clients can join on this switch port. 0 means no limit.

Default The default is 0, which means no limit

Mode Interface mode for a switch port

Usage notes We recommend using this command with IGMP snooping fast leave on the relevant VLANs. To enable fast leave, use the command:

```
awplus(config-if)# ip igmp snooping fast-leave
```

The device keeps count of the number of groups learned by each port. This counter is incremented when group joins are received via IGMP reports. It is decremented when:

- Group memberships time out
- Group leaves are received via leave messages or reports

Also, the port's group counter is cleared when:

- The port goes down
- You run the command **clear ip igmp group ***
- The port is removed from a VLAN

You can see the current value of the group counter by using either of the commands:

```
awplus# show ip igmp snooping statistics interface <port-list>
awplus# show ip igmp interface <port>
```

Example To limit clients to 10 groups on port 1.0.1, which is in vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# ip igmp maximum-groups 10
awplus(config-if)# exit
awplus(config)# interface vlan1
awplus(config-if)# ip igmp snooping fast-leave
```

Related commands

clear ip igmp group

ip igmp snooping fast-leave

show ip igmp interface

show ip igmp snooping statistics

ip igmp mroute-proxy

Overview Use this command to enable IGMP mroute proxy on this downstream interface and associate it with the upstream proxy service interface.

Use the **no** variant of this command to remove the association with the proxy-service interface.

Syntax

```
ip igmp mroute-proxy <interface>
no ip igmp mroute-proxy
```

Parameter	Description
<interface>	The name of the interface.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to VLAN interfaces configured for IGMP Proxy.

You must also enable the IGMP proxy service on the upstream interface, using the ip igmp proxy-service command. You can associate one or more downstream mroute proxy interfaces on the device with a single upstream proxy service interface. This downstream mroute proxy interface listens for IGMP reports, and forwards them to the upstream IGMP proxy service interface.

IGMP Proxy does not work with other multicast routing protocols, such as PIM-SM or PIM-DM.

Example To configure vlan2 as the upstream proxy-service interface for the downstream vlan3 interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip igmp mroute-proxy vlan2
```

Related commands ip igmp proxy-service

ip igmp proxy-service

Overview Use this command to enable the VLAN interface to be the upstream IGMP proxy-service interface for the device. All associated downstream IGMP mroute proxy interfaces on this device will have their memberships consolidated on this proxy service interface, according to IGMP host-side functionality.

Use the **no** variant of this command to remove the designation of the VLAN interface as an upstream proxy-service interface.

Syntax

```
ip igmp proxy-service
no ip igmp proxy-service
```

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to VLAN interfaces configured for IGMP Proxy.

This command is used with the ip igmp mroute-proxy command to enable forwarding of IGMP reports to a proxy service interface for all forwarding entries for this interface. You must also enable the downstream IGMP mroute proxy interfaces on this device using the command ip igmp mroute-proxy.

IGMP Proxy does not work with other multicast routing protocols, such as PIM-SM or PIM-DM.

From version 5.4.7-1.1 onwards, IGMP mroute proxy interfaces do not have to be configured with an IP address before they can operate. Instead, it is possible to have an address-less interface operate as an IGMP mroute proxy interface.

This feature is useful when IGMP Proxy needs to run on many downstream interfaces. For example, you may want to use it if your device has one subscriber (multicast receiver) per VLAN, and many receivers (many VLANs) connected to the device. In such a situation, assigning IP addresses to each VLAN may not be practicable.

Note that for such interface to be able to send queries to hosts directly attached to the interface, it is necessary to enable IGMP snooping querier on the interface, using the command ip igmp snooping querier.

Example To designate VLAN1 as the upstream proxy-service interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip igmp proxy-service
```

Related commands

ip igmp mroute-proxy

ip igmp snooping querier

Command changes

Version 5.4.7-1.1: Address-less interface support added.

Version 5.4.7-1.1: VRF-lite support added to SBx8100.

Version 5.4.8-1.1: VRF-lite support added to x930, SBx908 GEN2.

ip igmp querier-timeout

Overview Use this command to configure the timeout period before the device takes over as the querier for the interface after the previous querier has stopped querying.

Use the **no** variant of this command to restore the default.

Syntax

```
ip igmp querier-timeout <timeout>
no ip igmp querier-timeout
```

Parameter	Description
<timeout>	IGMP querier timeout interval value in seconds, in the range 1-65535.

Default The default timeout interval is 255 seconds.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to VLAN interfaces configured for IGMP.

The timeout value should not be less than the current active querier's general query interval.

Example To configure the device to wait 130 seconds from the time it received the last query before it takes over as the querier for vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp querier-timeout 130
```

Related commands

ip igmp query-interval

show ip igmp interface

show running-config

ip igmp query-holdtime

Overview This command sets the time that an IGMP Querier waits after receiving a query solicitation before it sends an IGMP Query. IGMP General Query messages will not be sent during the hold time interval.

Use the **no** variant of this command to return to the default query hold time period.

Syntax

```
ip igmp query-holdtime <interval>
no ip igmp query-holdtime
```

Parameter	Description
<interval>	Query interval value in milliseconds, in the range <100-5000>.

Default By default the delay before sending IGMP General Query messages is 500 milliseconds.

Mode Interface Configuration for a VLAN interface.

Usage notes Use this command to configure a value for the IGMP query hold time in the current network. IGMP Queries can be generated after receiving Query Solicitation (QS) packets and there is a possibility of a DoS (Denial of Service) attack if a stream of Query Solicitation (QS) packets are sent to the IGMP Querier, eliciting a rapid stream of IGMP Queries. This command applies to interfaces on which the device is acting as an IGMP Querier.

Use the ip igmp query-interval command when a delay for IGMP general query messages is required and IGMP general query messages are required. The **ip igmp query-holdtime** command stops IGMP query messages during the configured holdtime interval, so the rate of IGMP Queries that can be sent out of an interface can be restricted.

See the IGMP Feature Overview and Configuration Guide for introductory information about the Query Solicitation feature.

Examples To set the IGMP query holdtime to 900 ms for vlan20, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp query-holdtime 900
```

To reset the IGMP query holdtime to the default (500 ms) for vlan10, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip igmp query-holdtime
```

Related commands

ip igmp query-interval

ip igmp snooping tcn query solicit

show ip igmp interface

show running-config

ip igmp query-interval

Overview Use this command to configure the period for sending IGMP General Query messages.

The IGMP query interval specifies the time between IGMP General Query messages being sent.

Use the **no** variant of this command to return to the default query interval period.

NOTE: *The IGMP query interval must be greater than IGMP query maximum response time.*

Syntax

```
ip igmp query-interval <interval>
no ip igmp query-interval
```

Parameter	Description
<interval>	Query interval value in seconds, in the range <2-18000>.

Default The default IGMP query interval is 125 seconds.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to interfaces configured for IGMP. Note that the IGMP query interval is automatically set to a greater value than the IGMP query max response time.

For example, if you set the IGMP query max response time to 2 seconds using the ip igmp query-max-response-time command, and the IGMP query interval is currently less than 3 seconds, then the IGMP query interval period will be automatically reconfigured to be 3 seconds, so it is greater than the IGMP query maximum response time.

Use the **ip igmp query-interval** command when a non-default interval for IGMP General Query messages is required.

The ip igmp query-holdtime command can occasionally delay the sending of IGMP Queries.

Examples To set the period between IGMP host-query messages to 3 minutes (180 seconds) for vlan20, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp query-interval 180
```

To reset the period between sending IGMP host-query messages to the default (125 seconds) for vlan10, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip igmp query-interval
```

Related commands

ip igmp query-holdtime

ip igmp query-max-response-time

ip igmp startup-query-interval

show ip igmp interface

show running-config

ip igmp query-max-response-time

Overview Use this command to configure the maximum response time advertised in IGMP Queries.

Use the **no** variant of this command to restore the default.

NOTE: *The IGMP query maximum response time must be less than the IGMP query interval.*

Syntax

```
ip igmp query-max-response-time <response-time>
no ip igmp query-max-response-time
```

Parameter	Description
<response-time>	Response time value in seconds, in the range 1-3180.

Default The default IGMP query maximum response time is 10 seconds.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to interfaces configured for IGMP.

Note that the IGMP query interval is automatically set to a greater value than the IGMP query maximum response time.

For example, if you set the IGMP query interval to 3 seconds using the ip igmp query-interval command, and the current IGMP query interval is less than 3 seconds, then the IGMP query maximum response time will be automatically reconfigured to be 2 seconds, so it is less than the IGMP query interval time.

To get the network to converge faster, use the **ip igmp query-max-response-time** command and set a low response time value, such as one or two seconds, so that the clients will respond immediately with a report as a response to the IGMP Queries.

Examples To set a maximum response time of 8 seconds for vlan20, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp query-max-response-time 8
```

To reset the default maximum response time to the default (10 seconds) for vlan10, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip igmp query-max-response-time
```

Related commands

ip igmp query-interval

show ip igmp interface

show running-config

ip igmp ra-option

Overview Use this command to enable strict Router Alert (RA) option validation. With strict RA option enabled, IGMP packets without RA options are ignored.

Use the **no** variant of this command to disable strict RA option validation.

Syntax

```
ip igmp ra-option
no ip igmp ra-option
```

Default The default state of RA validation is unset.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to interfaces configured for IGMP and IGMP Snooping.

Examples To enable strict Router Alert (RA) option validation on vlan20, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp ra-option
```

ip igmp robustness-variable

Overview Use this command to change the robustness variable value on an interface.

Use the **no** variant of this command to return to the default on an interface.

Syntax

```
ip igmp robustness-variable <1-7>
no ip igmp robustness-variable
```

Parameter	Description
<1-7>	The robustness variable value.

Default The default robustness variable value is 2.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to interfaces configured for IGMP and IGMP Snooping.

Examples To set the robustness variable to 3 on vlan20, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp robustness-variable 3
```

Related commands

show ip igmp interface

show running-config

ip igmp snooping

Overview Use this command to enable IGMP Snooping. When this command is used in the Global Configuration mode, IGMP Snooping is enabled at the device level. When this command is used in Interface Configuration mode, IGMP Snooping is enabled for the specified VLANs.

Use the **no** variant of this command to either globally disable IGMP Snooping, or disable IGMP Snooping on a specified interface.

NOTE: *IGMP snooping cannot be disabled on an interface if IGMP snooping has already been disabled globally. IGMP snooping can be disabled on both an interface and globally if disabled on the interface first and then disabled globally.*

Syntax

```
ip igmp snooping
no ip igmp snooping
```

Default By default, IGMP Snooping is enabled both globally and on all VLANs.

Mode Global Configuration and Interface Configuration for a VLAN interface.

Usage notes For IGMP snooping to operate on particular VLAN interfaces, it must be enabled both globally by using this command in Global Configuration mode, and on individual VLAN interfaces by using this command in Interface Configuration mode (both are enabled by default.)

Both IGMP snooping and MLD snooping must be enabled globally on the device for IGMP snooping to operate. MLD snooping is also enabled by default. To enable it if it has been disabled, use the ipv6 mld snooping command in Global Configuration mode.

Examples To enable IGMP Snooping on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# ip igmp snooping
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping
```

Related commands

ipv6 mld snooping

show ip igmp interface

show running-config

ip igmp snooping fast-leave

Overview Use this command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing. The IGMP group-membership entry is removed as soon as an IGMP leave group message is received, without sending out a group-specific query.

Use the **no** variant of this command to disable fast-leave processing.

Syntax
```
ip igmp snooping fast-leave
no ip igmp snooping fast-leave
```

Default IGMP Snooping fast-leave processing is disabled.

Mode Interface Configuration for a VLAN interface.

Usage notes This IGMP Snooping command can only be configured on VLAN interfaces.

Example To enable fast-leave processing on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping fast-leave
```

Related commands show ip igmp interface

show running-config

ip igmp snooping mrouter

Overview Use this command to statically configure the specified port as a multicast router port for IGMP Snooping for an interface. This command applies to interfaces configured for IGMP Snooping.

Use the **no** variant of this command to remove the static configuration of the port as a multicast router port.

Syntax

```
ip igmp snooping mrouter interface <port>
no ip igmp snooping mrouter interface <port>
```

Parameter	Description
<port>	The port may be a device port (e.g. port1.0.2), a static channel group (e.g. sa3), or a dynamic (LACP) channel group (e.g. po4).

Mode Interface Configuration for a VLAN interface.

Example To configure port1.0.2 statically as a multicast router interface for vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping mrouter interface port1.0.2
```

Related commands show ip igmp snooping mrouter

ip igmp snooping querier

Overview Use this command to enable IGMP querier operation when no multicast routing protocol is configured. When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces. This command applies to interfaces configured for IGMP Snooping.

Use the **no** variant of this command to disable IGMP querier configuration.

Syntax

```
ip igmp snooping querier
no ip igmp snooping querier
```

Mode Interface Configuration for a VLAN interface.

Usage notes The IGMP Snooping querier uses the `0.0.0.0` Source IP address because it only masquerades as a proxy IGMP querier for faster network convergence.

It does not start, or automatically cease, the IGMP Querier operation if it detects query message(s) from a multicast router.

If an IP address is assigned to a VLAN, which has IGMP querier enabled on it, then the IGMP Snooping querier uses the VLAN's IP address as the Source IP Address in IGMP queries.

The IGMP Snooping Querier will not stop sending IGMP Queries if there is another IGMP Snooping Querier in the network with a lower Source IP Address.

NOTE: *Do not enable the IGMP Snooping Querier feature on a Layer 2 device when there is an operational IGMP Querier in the network.*

Example To configure vlan2 as a Snooping querier, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping querier
```

Related commands

show ip igmp interface

show running-config

ip igmp snooping report-suppression

Overview Use this command to enable report suppression for IGMP versions 1 and 2. This command applies to interfaces configured for IGMP Snooping.

Report suppression stops reports being sent to an upstream multicast router port when there are already downstream ports for this group on this interface.

Use the **no** variant of this command to disable report suppression.

Syntax

```
ip igmp snooping report-suppression
no ip igmp snooping report-suppression
```

Default Report suppression does not apply to IGMPv3, and is turned on by default for IGMPv1 and IGMPv2 reports.

Mode Interface Configuration for a VLAN interface.

Example To enable report suppression for IGMPv2 reports for vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp version 2
awplus(config-if)# ip igmp snooping report-suppression
```

Related commands show ip igmp interface

show running-config

ip igmp snooping routermode

Overview Use this command to set the destination IP addresses as router multicast addresses.

Use the **no** variant of this command to set it to the default. You can also remove a specified IP address from a custom list of multicast addresses.

Syntax

```
ip igmp snooping routermode
{all|default|ip|multicastrouter|address <ip-address>}
```

```
no ip igmp snooping routermode [address <ip-address>]
```

Parameter	Description
`all`	All reserved multicast addresses (224.0.0.x). Packets from all possible addresses in range 224.0.0.x are treated as coming from routers.
`default`	Default set of reserved multicast addresses. Packets from 224.0.0.1, 224.0.0.2, 224.0.0.4, 224.0.0.5, 224.0.0.6, 224.0.0.9, 224.0.0.13, 224.0.0.15 and 224.0.0.24 are treated as coming from routers.
`ip`	Custom reserved multicast addresses. Packets from custom IP address in the 224.0.0.x range are treated as coming from routers.
`multicastrouter`	Packets from DVMRP (224.0.0.4) and PIM (224.0.0.13) multicast addresses are treated as coming from routers.
`address <ip-address>`	Packets from the specified multicast address are treated as coming from routers. The address must be in the 224.0.0.x range.

Default The default routermode is **default** (not **all**) and shows the following reserved multicast addresses:

```
Router mode.............Def

Reserved multicast address
         224.0.0.1
         224.0.0.2
         224.0.0.4
         224.0.0.5
         224.0.0.6
         224.0.0.9
         224.0.0.13
         224.0.0.15
         224.0.0.24
```

Mode Global Configuration

Examples

To set **ip igmp snooping routermode** for all default reserved addresses enter:

```
awplus(config)# ip igmp snooping routermode default
```

To remove the multicast address 224.0.0.5 from the custom list of multicast addresses enter:

```
awplus(config)# no ip igmp snooping routermode address
224.0.0.5
```

Related commands

ip igmp trusted

show ip igmp snooping routermode

Command changes

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip igmp snooping source-timeout

Overview Use this command to set the global IGMP Snooping source time-out value (in seconds) on the switch.

Use the **no** variant of this command to set the source time-out value to be the same as the group membership timeout.

Syntax

```
ip igmp snooping source-timeout <timeout>
no ip igmp snooping source-timeout <timeout>
```

Parameter	Description
<timeout>	Time-out value in seconds *<0-86400>*

Default Global IGMP Snooping source-timeout is disabled by default, and unregistered multicast will be timed-out like normal entries.

Interface IGMP Snooping source timeout is disabled by default, and unregistered multicast will be timed-out like normal entries.

Mode Interface/Global Configuration

Usage notes The timeout determines how long unregistered multicast entries will be kept for. If the value '0' is specified, then effectively all unregistered multicast entries will never be timed out, and can only be cleared by using the command **clear ip igmp group**. The interface settings will always take precedence over the global setting.

Example To configure IGMP Snooping source timeout on 'vlan1', use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip igmp snooping source-timeout 200
```

Related commands show ip igmp snooping source-timeout

ip igmp snooping tcn query solicit

Overview Use this command to enable IGMP (Internet Group Management Protocol) Snooping TCN (Topology Change Notification) Query Solicitation feature. When this command is used in the Global Configuration mode, Query Solicitation is enabled.

Use the **no** variant of this command to disable IGMP Snooping TCN Query Solicitation. When the **no** variant of this command is used in Interface Configuration mode, this overrides the Global Configuration mode setting and Query Solicitation is disabled.

Syntax

```
ip igmp snooping tcn query solicit
no ip igmp snooping tcn query solicit
```

Default IGMP Snooping TCN Query Solicitation is disabled by default on the device, unless the device is the Master Node in an EPSR ring, or is the Root Bridge in a Spanning Tree.

When the device is the Master Node in an EPSR ring, or the device is the Root Bridge in a Spanning Tree, then IGMP Snooping TCN Query Solicitation is enabled by default and cannot be disabled using the Global Configuration mode command. However, Query Solicitation can be disabled for specified interfaces using the **no** variant of this command from the Interface Configuration mode.

Mode Global Configuration, and Interface Configuration for a VLAN interface.

Usage notes Once enabled, if the device is not an IGMP Querier, on detecting a topology change, the device generates IGMP Query Solicit messages that are sent to all the ports of the vlan configured for IGMP Snooping on the device.

On a device that is not the Master Node in an EPSR ring or the Root Bridge in a Spanning Tree, Query Solicitation can be disabled using the **no** variant of this command after being enabled.

If the device that detects a topology change is an IGMP Querier then the device will generate an IGMP Query message.

Note that the **no** variant of this command when issued in Global Configuration mode has no effect on a device that is the Master Node in an EPSR ring or on a device that is a Root Bridge in a Spanning Tree. Query Solicitation is not disabled for the device these instances. However, Query Solicitation can be disabled on a per-vlan basis from the Interface Configuration mode.

See the following state table that shows when Query Solicit messages are sent in these instances:

Command issued from Global Configuration	Command issued from Interface Configuration	Device is STP Root Bridge or the EPSR Master Node	IGMP Query Solicit message sent on VLAN
No	Yes	Yes	Yes
Yes	No	Yes	No
Yes	Yes	Yes	Yes

See the IGMP Feature Overview and Configuration Guide for introductory information about the Query Solicitation feature.

Examples To enable Query Solicitation on a device, use the commands:

```
awplus# configure terminal
awplus(config)# ip igmp snooping tcn query solicit
```

To disable Query Solicitation on a device, use the commands:

```
awplus# configure terminal
awplus(config)# no ip igmp snooping tcn query solicit
```

To enable Query Solicitation for vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping tcn query solicit
```

To disable Query Solicitation for vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip igmp snooping tcn query solicit
```

Related commands

ip igmp query-holdtime

show ip igmp interface

show running-config

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip igmp source-address-check

Overview This command enables the checking of the Source Address for an IGMP Report, rejecting any IGMP Reports originating on devices outside of the local subnet.

Use the **no** variant of this command to disable the checking of the Source Address for an IGMP Report, which allows IGMP Reports from devices outside of the local subnet.

Syntax

```
ip igmp source-address-check
no ip igmp source-address-check
```

Default Source address checking for IGMP Reports is enabled by default.

Mode Interface Configuration for a VLAN interface.

Usage notes This is a security feature, and should be enabled unless IGMP Reports from outside the local subnet are expected, for example, if Multicast VLAN Registration is active in the network.

The no variant of this command is required to disable the IGMP Report source address checking feature in networks that use Multicast VLAN Registration to allow IGMP Reports from devices outside of the local subnet.

Examples To deny IGMP Reports from outside the current subnet for vlan20, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp source-address-check
```

To allow IGMP Reports from outside the current subnet for vlan10, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip igmp source-address-check
```

Validation Commands show ip igmp interface

show running-config

ip igmp ssm

Overview Use this command to define a non-default Source Specific Multicast (SSM) range of IP multicast addresses in IGMP. Incoming IGMPv1 and IGMPv2 join requests are ignored if the multicast IP address is in the SSM range and no SSM mapping is configured for these addresses. By default, the SSM range is 232/8. To define the SSM range to be other than the default, use one of the access-list parameter options.

Use the **no** variant of this command to change the SSM range in IGMP back to the default.

Syntax

```
ip igmp ssm range {<access-list-number>|<access-list-name>}
no ip igmp ssm
```

Parameter	Description
<access-list-number>	Access-list number, in the range 1 to 99.
<access-list-name>	Standard IP access-list name.

Default By default the SSM range is 232/8.

Mode Global Configuration

Examples To configure a non-default SSM range to be used in IGMP enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 10 permit 224.1.1.0 0.0.0.255
awplus(config)# ip igmp ssm range 10
```

To return to the default configuration enter the commands:

```
awplus# configure terminal
awplus(config)# no ip igmp ssm
```

Related commands access-list (standard numbered)

ip pim ssm

ip igmp ssm-map enable

Overview Use this command to enable Source Specific Multicast (SSM) mapping on the device.

Use the **no** variant of this command to disable SSM mapping.

Syntax

```
ip igmp ssm-map enable
no ip igmp ssm-map enable
```

Mode Global Configuration

Usage notes This command applies to VLAN interfaces configured for IGMP.

Example To enable SSM on the device enter the commands:

```
awplus# configure terminal
awplus(config)# ip igmp ssm-map enable
```

Related commands ip igmp ssm-map static

ip igmp ssm-map static

Overview Use this command to specify the static mode of defining Source Specific Multicast (SSM) mapping. SSM statically assigns sources to IGMPv1 and IGMPv2 groups to translate such (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM.

Use the **no** variant of this command to remove the SSM map association.

Syntax

```
ip igmp ssm-map static
{<access-list-number>|<access-list-number-extended>|
<access-list-name>} <ip-address>
```

```
no ip igmp ssm-map static
{<access-list-number>|<access-list-number-extended>|
<access-list-name>} <ip-address>
```

Parameter	Description
<access-list-number>	Access-list number, in the range 1 to 99.
<access-list-number-extended>	Access-list number (expanded range), in the range 1300 to 1999.
<access-list-name>	Standard IP access-list name.
<ip-address>	Source address to use for static map group, entered in the form A.B.C.D.

Mode Global Configuration

Usage notes This command applies to VLAN interfaces configured for IGMP. You can use Standard numbered and Standard named ACLs plus Expanded Numbered ACLs.

Examples This example shows how to configure an SSM static mapping for group-address `224.1.1.1`, using a standard numbered ACL shown as `10`:

```
awplus# configure terminal
awplus(config)# access-list 10 permit 224.1.1.1 0.0.0.0
awplus(config)# ip igmp ssm-map static 10 1.2.3.4
```

This example shows how to configure an SSM static mapping for group-address `224.1.1.1`, using an expanded numbered ACL shown as `1301`:

```
awplus# configure terminal
awplus(config)# access-list 1301 permit 224.1.1.1 0.0.0.0
awplus(config)# ip igmp ssm-map static 1301 1.2.3.4
```

This example shows how to configure an SSM static mapping for group-address `224.1.1.1`, using a standard named ACL shown as `sales`:

```
awplus# configure terminal
awplus(config)# access-list sales permit 224.1.1.1 0.0.0.0
awplus(config)# ip igmp ssm-map static sales 1.2.3.4
```

Related commands ip igmp ssm-map enable

ip igmp static-group

Overview Use this command to statically configure multicast group membership entries on a VLAN interface, or to statically forward a multicast channel out a particular port or port range.

To statically add only a group membership, do not specify any parameters.

To statically add a (*,g) entry to forward a channel out of a port, specify only the multicast group address and the switch port range.

To statically add an (s,g) entry to forward a channel out of a port, specify the multicast group address, the source IP address, and the switch port range.

To use Source Specific Multicast mapping to determine the source IP address of the multicast server use the **ssm-map** parameter instead of specifying the source IP address.

Use the **no** variant of this command to delete static group membership entries.

Syntax

```
ip igmp static-group <ip-address> [source
{<ip-source-addr>|ssm-map}] [interface <port>]
```

```
no ip igmp static-group <ip-address> [source
{<ip-source-addr>|ssm-map}] [interface <port>]
```

Parameter	Description
<ip-address>	Standard IP Multicast group address, entered in the form A.B.C.D, to be configured as a static group member.
source	Optional.
<ip-source-addr>	Standard IP source address, entered in the form A.B.C.D, to be configured as a static source from where multicast packets originate.
ssm-map	This parameter uses Source Specific Multicast (SSM) Mapping to determine the source IP address associated with the specified IP Multicast group address. SSM mappings are configured using the ip igmp ssm-map static command.
interface	Use this parameter to specify a specific switch port or switch port range to statically forward the multicast group out of. If not used, static configuration is applied on all ports in the VLAN.
<port>	The port or port range to statically forward the group out of. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2).

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to IGMP operation, or to IGMP Snooping on a VLAN interface.

Example The following example show how to statically add group and source records for IGMP on vlan3:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip igmp
awplus(config-if)# ip igmp static-group 226.1.2.4 source
10.2.3.4
```

ip igmp startup-query-count

Overview Use this command to configure the IGMP startup query count for an interface. The IGMP startup query count is the number of IGMP General Query messages sent by a querier at startup. The default IGMP startup query count is 2.

Use the **no** variant of this command to return an interface's configured IGMP startup query count to the default.

Syntax

```
ip igmp startup-query-count <startup-query-count>
no ip igmp startup-query-count
```

Parameter	Description
<startup-query-count>	Specify the IGMP startup query count, in the range 2-10.

Default The default IGMP startup query count is 2.

Mode Interface Configuration for a VLAN interface.

Example To set the IGMP startup query count to `4` on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp startup-query-count 4
```

Related commands ip igmp last-member-query-count

ip igmp startup-query-interval

ip igmp startup-query-interval

Overview Use this command to configure the IGMP startup query interval for an interface. The IGMP startup query interval is the amount of time in seconds between successive IGMP General Query messages sent by a querier during startup. The default IGMP startup query interval is one quarter of the IGMP query interval value.

Use the **no** variant of this command to return an interface's configured IGMP startup query interval to the default.

Syntax

```
ip igmp startup-query-interval <startup-query-interval>
no ip igmp startup-query-interval
```

Parameter	Description
<startup-query-interval>	Specify the IGMP startup query interval, in the range of 2-1800 seconds. The value must be one quarter of the IGMP query interval value.

Default The default IGMP startup query interval is one quarter of the IGMP query interval value.

NOTE: *The IGMP startup query interval must be one quarter of the IGMP query interval.*

Mode Interface Configuration for a VLAN interface.

Example To set the IGMP startup query interval to 15 seconds for vlan2, which is one quarter of the IGMP query interval of 60 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp query-interval 60
awplus(config-if)# ip igmp startup-query-interval 15
```

Related commands

ip igmp last-member-query-interval

ip igmp query-interval

ip igmp startup-query-count

ip igmp trusted

Overview Use this command to allow IGMP to process packets received on certain trusted ports only.

Use the **no** variant of this command to stop IGMP from processing specified packets if the packets are received on the specified ports or aggregator.

Syntax

```
ip igmp trusted {all|query|report|routermode}
no ip igmp trusted {all|query|report|routermode}
```

Parameter	Description
`all`	Specifies whether or not the interface is allowed to receive all IGMP and other routermode packets
`query`	Specifies whether or not the interface is allowed to receive IGMP queries
`report`	Specifies whether or not the interface is allowed to receive IGMP membership reports
`routermode`	Specifies whether or not the interface is allowed to receive routermode packets

Default By default, all ports and aggregators are trusted interfaces, so IGMP is allowed to process all IGMP query, report, and router mode packets arriving on all interfaces.

Mode Interface mode for one or more switch ports or aggregators

Usage Because all ports are trusted by default, use this command in its **no** variant to stop IGMP processing packets on ports you do not trust.

For example, you can use this command to make sure that only ports attached to approved IGMP routers are treated as router ports.

Example To stop ports port1.0.3-port1.0.6 from being treated as router ports by IGMP, use the commands:

```
awplus(config)# interface port1.0.3-port1.0.6
awplus(config-if)# no ip igmp trusted routermode
```

Related commands ip igmp snooping routermode

ip igmp version

Overview Use this command to set the current IGMP version (IGMP version 1, 2 or 3) on an interface.

Use the **no** variant of this command to return to the default version.

Syntax

```
ip igmp version <1-3>
no ip igmp version
```

Parameter	Description
`version <1-3>`	IGMP protocol version number

Default The default IGMP version is 3.

Mode Interface Configuration for a VLAN interface.

Example To set the IGMP version to 2 for vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp version 2
```

Related commands show ip igmp interface

show debugging igmp

Overview Use this command to see what debugging is turned on for IGMP.

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

Syntax

```
show debugging igmp
```

Mode User Exec and Privileged Exec

Example To display the IGMP debugging options set, enter the command:

```
awplus# show debugging igmp
```

Output Figure 32-2: Example output from the **show debugging igmp** command

```
IGMP Debugging status:
  IGMP Decoder debugging is on
  IGMP Encoder debugging is on
  IGMP Events debugging is on
  IGMP FSM debugging is on
  IGMP Tree-Info-Base (TIB) debugging is on
```

Related commands debug igmp

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip igmp groups

Overview Use this command to display the multicast groups with receivers directly connected to the router, and learned through IGMP.

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

Syntax `show ip igmp groups [<ip-address>|<interface> detail | brief]`

Parameter	Description
<ip-address>	Address of the multicast group, entered in the form A.B.C.D.
<interface>	Interface name for which to display local information.
`brief`	Brief display of all interfaces

Mode User Exec and Privileged Exec

Example The following command displays local-membership information for all ports in all interfaces:

```
awplus# show ip igmp groups
```

Output Figure 32-3: Example output from **show ip igmp groups**

```
IGMP Connected Group Membership
Group Address    Interface       Uptime    Expires   Last Reporter
224.0.1.1        port1.0.1       00:00:09  00:04:17  10.10.0.82
224.0.1.24       port1.0.2       00:00:06  00:04:14  10.10.0.84
...
```

Table 32-1: Parameters in the output of **show ip igmp groups**

Parameter	Description
`Group Address`	Address of the multicast group.
`Interface`	Port through which the group is reachable.
`Uptime`	The time in weeks, days, hours, minutes, and seconds that this multicast group has been known to the device.
`Expires`	Time (in hours, minutes, and seconds) until the entry expires.
`Last Reporter`	Last host to report being a member of the multicast group.

Command changes

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

Version 5.4.8-2.3: **brief** parameter added.

show ip igmp interface

Overview Use this command to display the state of IGMP, IGMP Proxy service, and IGMP Snooping for a specified VLAN, or all VLANs. IGMP is shown as Active or Disabled in the show output. You can also display the number of groups a switch port belongs to.

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

Syntax

```
show ip igmp interface [<interface>]
```

Parameter	Description
<interface>	The name of the interface. If you specify a switch port number, the output displays the number of groups the port belongs to, and the port's group membership limit, if a limit has been set (with the command ip igmp maximum-groups).

Mode User Exec and Privileged Exec

Output The following output shows IGMP interface status for vlan2 with IGMP Snooping enabled:

```
awplus#show ip igmp interface vlan2
Interface vlan2 (Index 202)
 IGMP Disabled, Inactive, Version 3 (default)
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP robustness variable is 2
 IGMP last member query count is 2
 IGMP query interval is 125 seconds
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 Strict IGMPv3 ToS checking is disabled on this interface
 Source Address checking is enabled
 IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally disabled
  Num. query-solicit packets: 57 sent, 0 recvd
 IGMP Snooping is enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
```

The following output shows IGMP interface status for vlan2 with IGMP Snooping disabled:

```
awplus#show ip igmp interface vlan2
Interface vlan2 (Index 202)
 IGMP Disabled, Inactive, Version 3 (default)
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP robustness variable is 2
 IGMP last member query count is 2
 IGMP query interval is 125 seconds
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 Strict IGMPv3 ToS checking is disabled on this interface
 Source Address checking is enabled
 IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally disabled
  Num. query-solicit packets: 57 sent, 0 recvd
 IGMP Snooping is not enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
```

The following output displays membership information for port1.0.1:

```
awplus#show ip igmp interface port1.0.1
IGMP information for port1.0.1
    Maximum groups limit set: 10
    Number of groups port belongs to: 0
```

Command changes

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip igmp proxy

Overview Use this command to display the state of IGMP Proxy services for a specified interface or for all interfaces.

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

Syntax

```
show ip igmp proxy
```

Mode User Exec and Privileged Exec

Example To display the state of IGMP Proxy services for all interfaces, enter the command:

```
awplus# show ip igmp proxy
```

Output Figure 32-4: Example output from **show ip igmp proxy**

```
awplus#show ip igmp proxy
Interface vlan40 (Index 340)
Administrative status: enabled
Operational status: up
Upstream interface is vlan30
Number of multicast groups: 1
```

Related commands ip igmp proxy-service

show ip igmp proxy groups

Overview Use this command to display multicast groups with receivers directly connected to the router, learned through IGMP, which use a proxy service. You can also use a filter to specify a multicast group IP address and /or interface.

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

Syntax

```
show ip igmp proxy groups [detail]
show ip igmp proxy groups <multicast-group> [detail]
show ip igmp proxy groups <vlan> [detail]
show ip igmp proxy groups <vlan> <multicast-group> [detail]
```

Parameter	Description
`groups`	Specify IGMP proxy group membership information.
`detail`	Specify detailed IGMPv3 source information.
<vlan>	Specify the name of a single VLAN interface, for example **vlan1**.
<multicast-group>	Specify the IPv4 address in of the multicast group, in the format A.B.C.D.

Mode User Exec

Example To display local membership information for IGMP proxy service interfaces, use the command:

```
awplus# show ip igmp proxy groups
```

Output Figure 32-5: Example output from **show ip igmp proxy groups**

```
awplus#show ip igmp proxy groups
IGMP Connected Proxy Group Membership
Group Address    Interface            Member state
224.9.10.11      vlan10               Delay
```

Example To display local membership information for IGMP proxy service interfaces, use the command:

```
awplus# show ip igmp proxy groups detail
```

Output Figure 32-6: Example output from **show ip igmp proxy groups detail**

```
awplus#show ip igmp proxy groups detail
Interface:      vlan10
Group:          224.9.10.11
Group mode:     Exclude
Member state:   Delay
Source list is empty

Summary :
IGMP Connected Proxy Group Membership
Group Address    Interface            Member state
224.9.10.11      vlan10               DelayDetail :
Interface:       vlan10
Group:           224.9.10.11
Group mode:      Exclude
Member state:    Delay
Source list is empty
```

Table 32-2: Parameters in the output of **show ip igmp proxy groups**

Parameter	Description
`Interface`	The interface that received the IGMP report.
`Group`	The multicast group address that has been requested by the IGMP report.
`Group mode`	**Include**mode indicates that the multicast receiver has sent an IGMPv3 report for a group with a list of addresses that it wants to receive traffic from. **Exclude** mode indicates that the multicast receiver has sent an IGMPv3 report for a group with a list of addresses that it does not want to receive traffic from.
`Member state`	**Delay** indicates that no group or source query timers are running for the specified group, otherwise the member state is shown as **Idle**.

Related commands show ip igmp proxy

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip igmp snooping mrouter

Overview Use this command to display the multicast router ports, both static and dynamic, in a VLAN.

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

Syntax

```
show ip igmp snooping mrouter [interface <interface>]
```

Parameter	Description
`interface`	A specific interface.
`<interface>`	The name of the VLAN interface.

Mode User Exec and Privileged Exec

Example To show all multicast router interfaces, use the command:

```
awplus# show ip igmp snooping mrouter
```

To show the multicast router interfaces in `vlan1`, use the command:

```
awplus# show ip igmp snooping mrouter interface vlan1
```

Output Figure 32-7: Example output from **show ip igmp snooping mrouter**

```
VLAN    Interface   Static/Dynamic
1       port1.0.1   Statically configured
200     port1.0.2   Statically configured
```

Figure 32-8: Example output from **show ip igmp snooping mrouter interface vlan1**

```
VLAN    Interface   Static/Dynamic
1       port1.0.1   Statically configured
```

Related commands ip igmp snooping mrouter

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip igmp snooping routermode

Overview Use this command to display the current router mode and the list of IP addresses set as router multicast addresses from the ip igmp snooping routermode command.

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

Syntax

```
show ip igmp snooping routermode
```

Mode User Exec and Privileged Exec

Example To show the router mode and the list of router multicast addresses, use the command:

```
awplus# show ip igmp snooping routermode
```

Output Figure 32-9: Example output from **show ip igmp snooping routermode**

```
awplus#show ip igmp snooping routermode
Router mode.............Def
Reserved multicast address

         224.0.0.1
         224.0.0.2
         224.0.0.4
         224.0.0.5
         224.0.0.6
         224.0.0.9
         224.0.0.13
         224.0.0.15
         224.0.0.24
```

Related commands ip igmp snooping routermode

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip igmp snooping source-timeout

Overview Use this command to display the configured IGMP snooping source timeouts for a specified VLAN or VLAN range.

Syntax
```
show ip igmp snooping source-timeout [interface|
<interface-range>]
```

Parameter	Description
<interface-range>	The name of the VLAN interface or VLAN range

Mode Privileged Exec

Example To display the configured IGMP snooping source timeouts for all VLANs, use the command:

```
awplus# show ip igmp snooping source-timeout
```

Output Figure 32-10: Example output from **show ip igmp snooping source-timeout**

```
awplus#show ip igmp snooping source-timeout
Global IGMP snooping source-timeout is enabled (60 secs)

vlan1           enabled (300 secs)
vlan2           inherits global setting
vlan1000        inherits global settingawplus#show ip igmp
snooping source-timeout int vlan1
Global IGMP snooping source-timeout is enabled (60 secs)vlan1
enabled (300 secs)
```

Related commands ip igmp snooping source-timeout

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip igmp snooping statistics

Overview Use this command to display IGMP Snooping statistics data.

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

Syntax

```
show ip igmp snooping statistics interface <interface-range>
[group [<ip-address>]]
```

Parameter	Description
<ip-address>	Optionally specify the address of the multicast group, entered in the form A.B.C.D.
<interface>	Specify the name of the interface or interface range. If you specify a port number, the output displays the number of groups the port belongs to, and the port's group membership limit, if a limit has been set (with the command ip igmp maximum-groups)

Mode Privileged Exec

Example To display IGMP statistical information for **vlan1** and **vlan2**, use the command:

```
awplus# show ip igmp snooping statistics interface vlan1-vlan2
```

Output Figure 32-11: Example output from the **show ip igmp snooping statistics** command for VLANs

```
awplus#show ip igmp interface vlan1-vlan2
IGMP Snooping statistics for vlan1
Interface:      port1.0.1
Group:          224.1.1.1
Uptime:         00:00:09
Group mode:     Exclude (Expires: 00:04:10)
Last reporter:  10.4.4.5
Source list is empty
IGMP Snooping statistics for vlan2
Interface:      port1.0.2
Group:          224.1.1.2
Uptime:         00:00:19
Group mode:     Exclude (Expires: 00:05:10)
Last reporter:  10.4.4.6
Source list is empty
```

Figure 32-12: Example output from the **show ip igmp snooping statistics** command for a switch port

```
awplus#show ip igmp interface port1.0.1
IGMP information for port1.0.1
    Maximum groups limit set: 10
    Number of groups port belongs to: 0
```

Command changes

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

undebug igmp

Overview This command applies the functionality of the no debug igmp command.

33 MLD and MLD Snooping Commands

Introduction

Overview

This chapter provides an alphabetical reference of configuration, clear, and show commands related to MLD and MLD Snooping.

The Multicast Listener Discovery (MLD) module includes the MLD Proxy service and MLD Snooping functionality. Some of the following commands may have commonalities and restrictions; these are described under the Usage section for each command.

MLD and MLD Snooping commands only apply to switch ports, not Ethernet interfaces.

Before using PIM-SMv6:

- IPv6 must be enabled on an interface (ipv6 enable),
- IPv6 forwarding must be enabled globally for routing IPv6 (ipv6 forwarding), and
- IPv6 multicasting must be enabled globally (ipv6 multicast-routing).

Command List

- "clear ipv6 mld" on page 1682
- "clear ipv6 mld group" on page 1683
- "clear ipv6 mld interface" on page 1684
- "debug mld" on page 1685
- "ipv6 mld" on page 1686
- "ipv6 mld access-group" on page 1687
- "ipv6 mld immediate-leave" on page 1688
- "ipv6 mld last-member-query-count" on page 1689
- "ipv6 mld last-member-query-interval" on page 1690
- "ipv6 mld limit" on page 1691
- "ipv6 mld querier-timeout" on page 1693

- "ipv6 mld query-interval" on page 1694
- "ipv6 mld query-max-response-time" on page 1695
- "ipv6 mld robustness-variable" on page 1696
- "ipv6 mld snooping" on page 1697
- "ipv6 mld snooping fast-leave" on page 1699
- "ipv6 mld snooping mrouter" on page 1700
- "ipv6 mld snooping querier" on page 1702
- "ipv6 mld snooping report-suppression" on page 1703
- "ipv6 mld ssm-map enable" on page 1705
- "ipv6 mld ssm-map static" on page 1706
- "ipv6 mld static-group" on page 1707
- "ipv6 mld version" on page 1709
- "show debugging mld" on page 1710
- "show ipv6 mld groups" on page 1711
- "show ipv6 mld interface" on page 1712
- "show ipv6 mld snooping mrouter" on page 1713
- "show ipv6 mld snooping statistics" on page 1714

clear ipv6 mld

Overview Use this command to clear all MLD local memberships on all interfaces.

Syntax
```
clear ipv6 mld
```

Mode Privileged Exec

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols and learned by MLD Snooping.

Example
```
awplus# clear ipv6 mld
```

Related commands clear ipv6 mld group

clear ipv6 mld interface

clear ipv6 mld group

Overview Use this command to clear MLD specific local-membership(s) on all interfaces, for a particular group.

Syntax

```
clear ipv6 mld group {*|<ipv6-address>}
```

Parameter	Description
*	Clears all groups on all interfaces. This is an alias to the clear ipv6 mld command.
<ipv6-address>	Specify the group address for which MLD local-memberships are to be cleared from all interfaces. Specify the IPv6 multicast group address in the format in the format X:X::X:X.

Mode Privileged Exec

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols and learned by MLD Snooping.

Example

```
awplus# clear ipv6 mld group *
```

Related commands clear ipv6 mld

clear ipv6 mld interface

clear ipv6 mld interface

Overview Use this command to clear MLD interface entries.

Syntax

```
clear ipv6 mld interface <interface>
```

Parameter	Description
<interface>	Specifies name of the interface; all groups learned from this interface are deleted.

Mode Privileged Exec

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols and learned by MLD Snooping.

Example

```
awplus# clear ipv6 mld interface vlan2
```

Related commands clear ipv6 mld

clear ipv6 mld group

debug mld

Overview Use this command to enable all MLD debugging modes, or a specific MLD debugging mode.

Use the **no** variant of this command to disable all MLD debugging modes, or a specific MLD debugging mode.

Syntax

```
debug mld {all|decode|encode|events|fsm|tib}
no debug mld {all|decode|encode|events|fsm|tib}
```

Parameter	Description
`all`	Debug all MLD.
`decode`	Debug MLD decoding.
`encode`	Debug MLD encoding.
`events`	Debug MLD events.
`fsm`	Debug MLD Finite State Machine (FSM).
`tib`	Debug MLD Tree Information Base (TIB).

Mode Privileged Exec and Global Configuration

Usage notes This command applies to interfaces configured for MLD Layer 3 multicast protocols and learned by MLD Snooping.

Examples

```
awplus# configure terminal
awplus(config)# debug mld all
awplus# configure terminal
awplus(config)# debug mld decode
awplus# configure terminal
awplus(config)# debug mld encode
awplus# configure terminal
awplus(config)# debug mld events
```

Related commands show debugging mld

ipv6 mld

Overview Use this command to enable the MLD protocol operation on an interface. This command enables MLD protocol operation in stand-alone mode, and can be used to learn local-membership information prior to enabling a multicast routing protocol on the interface.

Use the **no** variant of this command to return all MLD related configuration to the default (including MLD Snooping).

NOTE: *There is a 100 MLD interface limit when applying MLD commands to multiple VLANs. Only the first 100 VLANs have the required multicast structures added to the interfaces that allow multicast routing.*

Syntax

```
ipv6 mld
no ipv6 mld
```

Default MLD is disabled by default.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage notes MLD requires memory for storing data structures, as well as the hardware tables to implement hardware routing. As the number of ports, VLANs, static and dynamic groups increases then more memory is consumed. You can track the memory used for MLD with the command:

```
awplus# show memory pools nsm | grep MLD
```

Static and dynamic groups (LACP), ports and VLANs are not limited for MLD. For VLANs, this allows you to configure MLD across more VLANs with fewer ports per VLAN, or fewer VLANs with more ports per VLAN. For LACPs, you can configure MLD across more LACP groups with fewer ports per LACP, or fewer LACP groups with more ports per LACP.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld
```

ipv6 mld access-group

Overview Use this command to control the multicast local-membership groups learned on an interface.

Use the **no** variant of this command to disable this access control.

Syntax

```
ipv6 mld access-group <IPv6-access-list-name>
no ipv6 mld access-group
```

Parameter	Description
<IPv6-access-list-name>	Specify a Standard or an Extended software IPv6 access-list name. See IPv6 Software Access Control List (ACL) Commands for supported IPv6 ACLs.

Default No access list is configured by default.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Examples In the following example, the VLAN interface `vlan2` will only accept MLD joins for groups in the range `ff1e:0db8:0001::/64`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard group1 permit
ff1e:0db8:0001::/64
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld access-group group1
```

In the following example, the VLAN interfaces `vlan2-vlan4` will only accept MLD joins for groups in the range `ff1e:0db8:0001::/64`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard group1 permit
ff1e:0db8:0001::/64
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld access-group group1
```

ipv6 mld immediate-leave

Overview Use this command to minimize the leave latency of MLD memberships.

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

Syntax

```
ipv6 mld immediate-leave group-list <IPv6-access-list-name>
no ipv6 mld immediate-leave
```

Parameter	Description
<IPv6-access-list-name>	Specify a Standard or an Extended software IPv6 access-list name that defines multicast groups in which the immediate leave feature is enabled. See IPv6 Software Access Control List (ACL) Commands for supported IPv6 ACLs.

Default Disabled

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Example The following example shows how to enable the immediate-leave feature on an interface for a specific range of multicast groups. In this example, the router assumes that the group access-list consists of groups that have only one node membership at a time per interface:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld immediate-leave v6grp
awplus(config-if)# exit
```

Related commands ipv6 mld last-member-query-interval

ipv6 mld last-member-query-count

Overview Use this command to set the last-member query-count value.

Use the **no** variant of this command to return to the default on an interface.

Syntax

```
ipv6 mld last-member-query-count <value>
no ipv6 mld last-member-query-count
```

Parameter	Description
<value>	Count value. Valid values are from `2 to 7`.

Default The default last-member query-count value is 2.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld last-member-query-count 3
```

ipv6 mld last-member-query-interval

Overview Use this command to configure the interval at which the router sends MLD group-specific host query messages.

Use the **no** variant of this command to set this frequency to the default.

Syntax

```
ipv6 mld last-member-query-interval <milliseconds>
no ipv6 mld last-member-query-interval
```

Parameter	Description
<milliseconds>	The time delay between successive query messages (in milliseconds). Valid values are from 1000 to 25500 milliseconds.

Default 1000 milliseconds

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Example The following example changes the MLD group-specific host query message interval to 2 seconds:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld last-member-query-interval 2000
```

Related commands ipv6 mld immediate-leave

ipv6 mld limit

Overview Use this command to configure a limit on the maximum number of group memberships that may be learned. The limit may be set for the device as a whole, or for a specific interface.

Once the specified group membership limit is reached, all further local-memberships will be ignored.

Optionally, an exception access-list can be configured to specify the group-address(es) that are exempted from being subject to the limit.

Use the **no** variant of this command to unset the limit and any specified exception access-list.

Syntax

```
ipv6 mld limit <limitvalue> [except <IPv6-access-list-name>]
no ipv6 mld limit
```

Parameter	Description
<limitvalue>	<2-512> Maximum number of group membership states.
<IPv6-access-list-name>	Specify a Standard or an Extended software IPv6 access-list name that defines multicast groups, which are exempted from being subject to the configured limit. See IPv6 Software Access Control List (ACL) Commands for supported IPv6 ACLs.

Default The default limit, which is reset by the **no** variant of this command, is the same as maximum number of group membership entries that can be learned with the **ipv6 mld limit** command.

The default limit of group membership entries that can be learned is 512 entries.

Mode Global Configuration and Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage notes This command applies to interfaces configured for MLD Layer-3 multicast protocols and learned by MLD Snooping.

Examples The following example configures an MLD limit of 100 group-memberships across all VLAN interfaces on which MLD is enabled, and excludes groups in the range `ff1e:0db8:0001::/64` from this limitation:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard v6grp permit
ff1e:0db8:0001::/64
awplus(config)# ipv6 mld limit 100 except v6grp
```

The following example configures an MLD limit of 100 group-membership states on the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld limit 100
```

The following example configures an MLD limit of 100 group-membership states on the VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld limit 100
```

Related commands

ipv6 mld immediate-leave

show ipv6 mld groups

ipv6 mld querier-timeout

Overview Use this command to configure the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

Use the **no** variant of this command to restore the default.

Syntax

```
ipv6 mld querier-timeout <seconds>
no ipv6 mld querier-timeout
```

Parameter	Description
<seconds>	Number of seconds that the router waits after the previous querier has stopped querying before it takes over as the querier. Valid values are from 2 to 65535 seconds.

Default 255 seconds

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage notes This command applies to interfaces configured for MLD Layer-3 multicast protocols.

Example The following example configures the router to wait 120 seconds from the time it received the last query before it takes over as the querier for the interface:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld querier-timeout 120
```

Related commands ipv6 mld query-interval

ipv6 mld query-interval

Overview Use this command to configure the frequency of sending MLD host query messages.

Use the **no** variant of this command to return to the default frequency.

Syntax

```
ipv6 mld query-interval <seconds>
no ipv6 mld query-interval
```

Parameter	Description
<seconds>	Variable that specifies the time delay between successive MLD host query messages (in seconds). Valid values are from `1 to 18000 seconds`.

Default The default query interval is 125 seconds.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols.

Example The following example changes the frequency of sending MLD host-query messages to 2 minutes:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld query-interval 120
```

Related commands ipv6 mld querier-timeout

ipv6 mld query-max-response-time

Overview Use this command to configure the maximum response time advertised in MLD queries.

Use the **no** variant of with this command to restore the default.

Syntax

```
ipv6 mld query-max-response-time <seconds>
no ipv6 mld query-max-response-time
```

Parameter	Description
<seconds>	Maximum response time (in seconds) advertised in MLD queries. Valid values are from 1 to 240 seconds.

Default 10 seconds

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols.

Example The following example configures a maximum response time of 8 seconds:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld query-max-response-time 8
```

ipv6 mld robustness-variable

Overview Use this command to change the robustness variable value on an interface.

Use the **no** variant of this command to return to the default on an interface.

Syntax

```
ipv6 mld robustness-variable <value>
no ipv6 mld robustness-variable
```

Parameter	Description
<value>	Valid values are from `1 to 7`.

Default The default robustness variable value is 2.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld robustness-variable 3
```

ipv6 mld snooping

Overview Use this command to enable MLD Snooping. When this command is issued in the Global Configuration mode, MLD Snooping is enabled globally for the device. When this command is issued in Interface mode for a VLAN then MLD Snooping is enabled for the specified VLAN. Note that MLD Snooping is enabled on the VLAN only if it is enabled globally and on the VLAN.

Use the **no** variant of this command to globally disable MLD Snooping in Global Configuration mode, or for the specified VLAN interface in Interface mode.

NOTE: *There is a 100 MLD interface limit when applying MLD commands to multiple VLANs. Only the first 100 VLANs have the required multicast structures added to the interfaces that allow multicast routing.*

Syntax

```
ipv6 mld snooping
no ipv6 mld snooping
```

Default By default, MLD Snooping is enabled both globally and on all VLANs.

Mode Global Configuration and Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage notes For MLD Snooping to operate on particular VLAN interfaces, it must be enabled both globally by using this command in Global Configuration mode, and on individual VLAN interfaces by using this command in Interface Configuration mode (both are enabled by default).

MLD requires memory for storing data structures, as well as the hardware tables to implement hardware routing. As the number of ports, VLANs, static and dynamic groups increases then more memory is consumed. You can track the memory used for MLD with the command:

```
awplus# show memory pools nsm | grep MLD
```

Static and dynamic groups (LACP), ports and VLANs are not limited for MLD. For VLANs, this allows you to configure MLD across more VLANs with fewer ports per VLAN, or fewer VLANs with more ports per VLAN. For LACPs, you can configure MLD across more LACP groups with fewer ports per LACP, or fewer LACP groups with more ports per LACP.

Examples To configure MLD Snooping on the VLAN interfaces `vlan2-vlan4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping
```

To disable MLD Snooping for the VLAN interfaces `vlan2-vlan4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config)# no ipv6 mld snooping
```

To configure MLD Snooping globally for the device, enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 mld snooping
```

To disable MLD Snooping globally for the device, enter the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 mld snooping
```

ipv6 mld snooping fast-leave

Overview Use this command to enable MLD Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing; the MLD group-membership is removed as soon as an MLD leave group message is received, without sending out a group-specific query.

Use the **no** variant of this command to disable fast-leave processing.

Syntax

```
ipv6 mld snooping fast-leave
no ipv6 mld snooping fast-leave
```

Default MLD Snooping fast-leave processing is disabled.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage notes This MLD Snooping command can only be configured on VLAN interfaces.

Examples This example shows how to enable fast-leave processing on the VLAN interface vlan2.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping fast-leave
```

This example shows how to enable fast-leave processing on the VLAN interface vlan2-vlan4.

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping fast-leave
```

ipv6 mld snooping mrouter

Overview Use this command to statically configure the specified port as a Multicast Router interface for MLD Snooping within the specified VLAN.

See detailed usage notes below to configure static multicast router ports when using static IPv6 multicast routes with EPSR, and the destination VLAN is an EPSR data VLAN.

Use the **no** variant of this command to remove the static configuration of the interface as a Multicast Router interface.

Syntax

```
ipv6 mld snooping mrouter interface <port>
no ipv6 mld snooping mrouter interface <port>
```

Parameter	Description
<port>	Specify the name of the port.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage notes This MLD Snooping command statically configures a switch port as a Multicast Router interface.

Note that if static IPv6 multicast routing is being used with EPSR and the destination VLAN is an EPSR data VLAN, then multicast router (mrouter) ports must be statically configured. This minimizes disruption for multicast traffic in the event of ring failure or restoration.

When configuring the EPSR data VLAN, statically configure mrouter ports so that the multicast router can be reached in either direction around the EPSR ring.

For example, if port1.0.1 and port1.0.6 are ports on an EPSR data VLAN vlan101, which is the destination for a static IPv6 multicast route, then configure both ports as multicast router (mrouter) ports as shown in the example commands listed below:

Figure 33-1: Example **ipv6 mld snooping mrouter** commands when static IPv6 multicast routing is being used and the destination VLAN is an EPSR data VLAN:

```
awplus>enable
awplus#configure terminal
awplus(config)#interface vlan101
awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.1
awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.6
```

Examples

This example shows how to specify the next-hop interface to the multicast router for VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping mrouter interface
port1.0.5
```

This example shows how to specify the next-hop interface to the multicast router for VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping mrouter interface
port1.0.5
```

Related commands

ipv6 multicast route

ipv6 mld snooping querier

Overview Use this command to enable MLD querier operation on a subnet (VLAN) when no multicast routing protocol is configured in the subnet (VLAN). When enabled, the MLD Snooping querier sends out periodic MLD queries for all interfaces on that VLAN.

Use the **no** variant of this command to disable MLD querier configuration.

Syntax

```
ipv6 mld snooping querier
no ipv6 mld snooping querier
```

Mode Interface Configuration for a specified VLAN interface.

Usage This command can only be configured on a single VLAN interface - not on multiple VLANs.

The MLD Snooping querier uses the 0.0.0.0 Source IP address because it only masquerades as an MLD querier for faster network convergence.

The MLD Snooping querier does not start, or automatically cease, the MLD Querier operation if it detects query message(s) from a multicast router. It restarts as an MLD Snooping querier if no queries are seen within the other querier interval.

Do not enable MLD Snooping querier if you have already enabled MLD on your device.

Do not enable MLD Snooping querier on your device and then enable MLD afterwards.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping querier
```

ipv6 mld snooping report-suppression

Overview Use this command to enable report suppression from hosts for Multicast Listener Discovery version 1 (MLDv1) on a VLAN in Interface Configuration mode.

Use the **no** variant of this command to disable report suppression on a VLAN in Interface Configuration mode.

Syntax

```
ipv6 mld snooping report-suppression
no ipv6 mld snooping report-suppression
```

Default Report suppression does not apply to MLDv2, and is turned on by default for MLDv1 reports.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This MLD Snooping command can only be configured on VLAN interfaces.

MLDv1 Snooping maybe configured to suppress reports from hosts. When a querier sends a query, only the first report for particular set of group(s) from a host will be forwarded to the querier by the MLD Snooping device. Similar reports (to the same set of groups) from other hosts, which would not change group memberships in the querier, will be suppressed by the MLD Snooping device to prevent 'flooding' of query responses.

Examples This example shows how to enable report suppression for MLD reports on VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping report-suppression
```

This example shows how to disable report suppression for MLD reports on VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 mld snooping report-suppression
```

This example shows how to enable report suppression for MLD reports on VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping report-suppression
```

This example shows how to disable report suppression for MLD reports on VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no ipv6 mld snooping report-suppression
```

ipv6 mld ssm-map enable

Overview Use this command to enable the Source Specific Multicast (SSM) mapping feature on the device.

Use the **no** variant of this command to disable the SSM mapping feature on the device.

Syntax

```
ipv6 mld ssm-map enable
no ipv6 mld ssm-map enable
```

Mode Global Configuration

Usage notes This command enables the SSM mapping feature for group members in the defined SSM range. Configure the group member and the SSM range using the ipv6 mld ssm-map static command.

Example This example shows how to enable the MLD SSM mapping feature on the device.

```
awplus# configure terminal
awplus(config)# ipv6 mld ssm-map enable
```

Related commands ipv6 mld ssm-map static

ipv6 mld ssm-map static

Overview Use this command to statically define a Source Specific Multicast (SSM) mapping. The SSM mapping statically assigns sources to MLDv1 groups to translate such (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM.

Use the **no** variant of this command to remove the SSM map association.

Syntax

```
ipv6 mld ssm-map static <access-list-name> X:X::X:X
no ipv6 mld ssm-map static <access-list-name> X:X::X:X
```

Parameter	Description
<access-list-name>	IPv6 named standard access-list.
X:X::X:X	IPv6 source address that is associated with the above access-list. The IPv6 address uses the format X:X::X:X.

Mode Global Configuration

Usage notes Use this command to configure SSM mappings after enabling SSM mapping with the ipv6 mld ssm-map enable command.

Example This example shows how to configure an SSM static mapping for the group-address ff0e::1/128.

```
awplus# configure terminal
awplus(config)# ipv6 mld ssm-map enable
awplus(config)# ipv6 access-list standard v6grp permit
ff0e::1/128
awplus(config)# ipv6 mld ssm-map static v6grp 2006::3
```

Related commands ipv6 mld ssm-map enable

ipv6 mld static-group

Overview Use this command to statically configure IPv6 group membership entries on an interface. To statically add only a group membership, do not specify any parameters.

Use the **no** variant of this command to delete static group membership entries.

Syntax

```
ipv6 mld static-group <ipv6-group-address> [source
<ipv6-source-address>|ssm-map] [interface <port>]
```

```
no ipv6 mld static-group <ipv6-group-address> [source
<ipv6-source-address>|ssm-map] [interface <port>]
```

Parameter	Description
<ipv6-group-address>	Specify a standard IPv6 Multicast group address to be configured as a static group member. The IPv6 address uses the format X:X::X:X.
<ipv6-source-address>	Optional. Specify a standard IPv6 source address to be configured as a static source from where multicast packets originate. The IPv6 address uses the format X:X::X:X.
`ssm-map`	Mode of defining SSM mapping. SSM mapping statically assigns sources to MLDv1 groups to translate these (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM.
<port>	Optional. Physical interface. This parameter specifies a physical port. If this parameter is used, the static configuration is applied to just to that physical interface. If this parameter is not used, the static configuration is applied on all ports in the VLAN.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to MLD Snooping on a VLAN interface to statically add groups and/or source records.

Examples To add a static group record, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10
```

To add a static group and source record, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
fe80::2fd:6cff:fe1c:b
```

To add a static group record on a specific port on vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 interface
port1.0.4
```

To add an SSM mapping record on a specific port on vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
ssm-map interface port1.0.4
```

ipv6 mld version

Overview Use this command to set the current MLD protocol version on an interface.

Use the **no** variant of this command to return to the default version on an interface.

Syntax

```
ipv6 mld version <version>
no ipv6 mld version
```

Parameter	Description
<version>	MLD protocol version number. Valid version numbers are 1 and 2

Default The default MLD protocol version number is 2.

Mode Interface Configuration for a VLAN interface.

Usage notes This command applies to interfaces configured for MLD Layer-3 multicast protocols and MLD Snooping. Note this command is intended for use where there is another querier (when there is another device with MLD enabled) on the same link that can only operate with MLD version 1. Otherwise, the default MLD version 2 is recommended for performance.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld version 1
```

show debugging mld

Overview Use this command to see what debugging is turned on for MLD. MLD debugging modes are enabled with the debug mld command.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax
```
show debugging mld
```

Mode Privileged Exec

Example
```
awplus# show debugging mld
```

Output
```
show debugging mld
MLD Debugging status:
  MLD Decoder debugging is on
  MLD Encoder debugging is on
  MLD Events debugging is on
  MLD FSM debugging is on
  MLD Tree-Info-Base (TIB) debugging is on
```

Related commands debug mld

show ipv6 mld groups

Overview Use this command to display the multicast groups that have receivers directly connected to the router and learned through MLD.

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

Syntax `show ipv6 mld groups [<ipv6-address>|<interface>] [detail]`

Parameter	Description
<ipv6-address>	Optional. Specify Address of the multicast group in format X:X::X:X.
<interface>	Optional. Specify the Interface name for which to display local information.

Mode User Exec and Privileged Exec

Examples The following command displays local-membership information for all interfaces:

```
awplus# show ipv6 mld groups
```

Output Figure 33-2: Example output for **show ipv6 mld groups**

```
awplus#show ipv6 mld groups
MLD Connected Group Membership
Group Address                           Interface            Uptime   Expires
                    Last Reporter
ff08::1                                 vlan10 (port1.0.1)   00:07:27 00:03:10
                    fe80::200:1ff:fe20:b5ac
```

The following command displays local-membership information for all interfaces:

```
awplus# show ipv6 mld groups detail
```

Output Figure 33-3: Example output for **show ipv6 mld groups detail**

```
MLD Connected Group Membership Details for port1.0.1
Interface:      port1.0.1
Group:          ff08::1
Uptime:         00:00:13
Group mode:     Include ()
Last reporter:  fe80::eecd:6dff:fe6b:4783
Group source list: (R - Remote, M - SSM Mapping, S - Static )
  Source Address                Uptime    v2 Exp    Fwd  Flags
  2001:db8::1                   00:00:13  00:04:07  Yes  R
  2002:db8::3                   00:00:13  00:04:07  Yes  R
```

show ipv6 mld interface

Overview Use this command to display the state of MLD and MLD Snooping for a specified interface, or all interfaces.

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

Syntax

```
show ipv6 mld interface [<interface>]
```

Parameter	Description
<interface>	Interface name.

Mode User Exec and Privileged Exec

Example The following command displays MLD interface status on all interfaces enabled for MLD:

```
awplus# show ipv6 mld interface
```

Output

```
awplus#show ipv6 mld interface

Interface vlan1 (Index 301)
 MLD Enabled, Active, Querier, Version 2 (default)
 Internet address is fe80::215:77ff:fec9:7468
 MLD interface has 0 group-record states
 MLD activity: 0 joins, 0 leaves
 MLD robustness variable is 2
 MLD last member query count is 2
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 MLD Snooping is globally enabled
 MLD Snooping is enabled on this interface
 MLD Snooping fast-leave is not enabled
 MLD Snooping querier is enabled
 MLD Snooping report suppression is enabled
```

show ipv6 mld snooping mrouter

Overview Use this command to display the multicast router interfaces, both configured and learned, in a VLAN. If you do not specify a VLAN interface then all the VLAN interfaces are displayed.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 mld snooping mrouter [<interface>]
```

Parameter	Description
<interface>	Optional. Specify the name of the VLAN interface. Note: If you do not specify a single VLAN interface, then all VLAN interfaces are shown.

Mode User Exec and Privileged Exec

Examples The following command displays the multicast router interfaces in `vlan2`:

```
awplus# show ipv6 mld snooping mrouter vlan2
```

Output

```
awplus#show ipv6 mld snooping mrouter vlan2
VLAN    Interface    Static/Dynamic
2       port1.0.2    Dynamically Learned
2       port1.0.3    Dynamically Learned
```

The following command displays the multicast router interfaces for all VLAN interfaces:

```
awplus# show ipv6 mld snooping mrouter
```

Output

```
awplus#show ipv6 mld snooping mrouter
VLAN    Interface    Static/Dynamic
2       port1.0.2    Dynamically Learned
2       port1.0.3    Dynamically Learned
3       port1.0.4    Statically Assigned
3       port1.0.5    Statically Assigned
```

show ipv6 mld snooping statistics

Overview Use this command to display MLD Snooping statistics data.

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

Syntax

```
show ipv6 mld snooping statistics interface <interface>
```

Parameter	Description
<interface>	The name of the VLAN interface.

Mode User Exec and Privileged Exec

Example The following command displays MLDv2 statistical information for `vlan1`:

```
awplus# show ipv6 mld snooping statistics interface vlan1
```

Output

```
awplus#show ipv6 mld snooping statistics interface vlan1
MLD Snooping statistics for vlan1
Interface:      port1.0.1
Group:          ff08::1
Uptime:         00:02:18
Group mode:     Include ()
Last reporter:  fe80::eecd:6dff:fe6b:4783
Group source list: (R - Remote, M - SSM Mapping, S - Static )
  Source Address       Uptime    v2 Exp    Fwd  Flags
  2001:db8::1          00:02:18  00:02:02  Yes  R
  2001:db8::3          00:02:18  00:02:02  Yes  R
```

34 Multicast Commands

Introduction

Overview This chapter provides an alphabetical reference of multicast commands for configuring:

- IPv4 and IPv6 multicast forwarding
- IPv4 and IPv6 static multicast routes
- mroutes (routes back to a multicast source)

For commands for other multicast protocols, see:

- IGMP and IGMP Snooping Commands
- MLD and MLD Snooping Commands
- PIM-SM Commands
- PIM-SMv6 Commands
- PIM-DM Commands

NOTE: *Before using PIM-SMv6 commands, IPv6 must be enabled on an interface with the ipv6 enable command, IPv6 forwarding must be enabled globally for routing IPv6 with the ipv6 forwarding command, and IPv6 multicasting must be enabled globally with the ipv6 multicast-routing command.*

Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the clear ipv6 mroute command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous static IPv6 multicast routes.

The IPv6 Multicast addresses shown can be derived from IPv6 unicast prefixes as per RFC 3306. The IPv6 unicast prefix reserved for documentation is 2001:0db8::/32 as per RFC 3849. Using the base /32 prefix the IPv6 multicast prefix for 2001:0db8::/32 is ff3x:20:2001:0db8::/64. Where an RP address is 2001:0db8::1 the embedded RP multicast prefix is ff7x:120:2001:0db8::/96.

The IPv6 addresses shown use the address space 2001:0db8::/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical

networks (other than for testing purposes) nor should they appear on any public network.

Command List

- "clear ip mroute" on page 1717
- "clear ip mroute statistics" on page 1718
- "clear ipv6 mroute" on page 1719
- "clear ipv6 mroute statistics" on page 1720
- "ipv6 multicast forward-slow-path-packet" on page 1721
- "debug nsm" on page 1722
- "debug nsm mcast" on page 1723
- "debug nsm mcast6" on page 1724
- "ip mroute" on page 1725
- "ip multicast allow-register-fragments" on page 1727
- "ip multicast forward-first-packet" on page 1728
- "ip multicast route" on page 1729
- "ip multicast route-limit" on page 1731
- "ip multicast wrong-vif-suppression" on page 1732
- "ip multicast-routing" on page 1733
- "ipv6 mroute" on page 1734
- "ipv6 multicast route" on page 1736
- "ipv6 multicast route-limit" on page 1739
- "ipv6 multicast-routing" on page 1740
- "multicast" on page 1741
- "platform multicast-ratelimit" on page 1742
- "show debugging nsm mcast" on page 1743
- "show ip mroute" on page 1744
- "show ip mvif" on page 1747
- "show ip rpf" on page 1748
- "show ipv6 mroute" on page 1749
- "show ipv6 multicast forwarding" on page 1751
- "show ipv6 mif" on page 1752

clear ip mroute

Overview Use this command to delete entries from the IPv4 multicast routing table.

NOTE: *If you use this command, you should also use the clear ip igmp group command to clear IGMP group membership records.*

Syntax

```
clear ip mroute {*|<ipv4-group-address>
[<ipv4-source-address>]} [pim sparse-mode]
```

Parameter	Description
*	Deletes all multicast routes.
<ipv4-group-address>	Group IPv4 address, in dotted decimal notation in the format A.B.C.D.
<ipv4-source-address>	Source IPv4 address, in dotted decimal notation in the format A.B.C.D.
pim sparse-mode	Clear specified IPv4 multicast route(s) for PIM Sparse Mode only.

Mode Privileged Exec

Usage notes When this command is used, the Multicast Routing Information Base (MRIB) clears the IPv4 multicast route entries in its IPv4 multicast route table, and removes the entries from the multicast forwarder. The MRIB sends a “clear” message to the multicast protocols. Each multicast protocol has its own “clear” multicast route command. The protocol-specific “clear” command clears multicast routes from PIM Sparse Mode, and also clears the routes from the MRIB.

Examples

```
awplus# clear ip mroute 225.1.1.1 192.168.3.3
awplus# clear ip mroute *
```

Related commands ip multicast route

show ip mroute

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

clear ip mroute statistics

Overview Use this command to delete multicast route statistics entries from the IP multicast routing table.

Syntax
```
clear ip mroute statistics {*|<ipv4-group-addr>
[<ipv4-source-addr>]}
```

Parameter	Description
*	All multicast route entries.
<ipv4-group-addr>	Group IPv4 address, in dotted decimal notation in the format A.B.C.D.
<ipv4-source-addr>	Source IPv4 address, in dotted decimal notation in the format A.B.C.D.

Mode Privileged Exec

Example
```
awplus# clear ip mroute statistics 225.1.1.2 192.168.4.4
awplus# clear ip mroute statistics *
```

clear ipv6 mroute

Overview Use this command to delete one or more dynamically-added route entries from the IPv6 multicast routing table.

You need to do this, for example, if you want to create a static route instead of an existing dynamic route.

Syntax

```
clear ipv6 mroute {*|<ipv6-group-address>
[<ipv6-source-address>]}
```

Parameter	Description
*	Deletes all dynamically-learned IPv6 multicast routes.
<ipv6-group-address>	Group IPv6 address, in hexadecimal notation in the format X.X::X.X.
<ipv6-source-address>	Source IPv6 address, in hexadecimal notation in the format X.X::X.X.

Mode Privileged Exec

Usage notes When this command is used, the Multicast Routing Information Base (MRIB) clears the relevant IPv6 multicast route entries in its IPv6 multicast route table, and removes the entries from the multicast forwarder. The MRIB sends a "clear" message to the multicast protocols. Each multicast protocol has its own "clear" multicast route command.

This command does not remove static routes from the routing table or the configuration. To remove static routes, use the **no** parameter of the command ipv6 multicast route.

Example

```
awplus# clear ipv6 mroute 2001::2 ff08::1
```

Related commands ipv6 multicast route

show ipv6 mroute

clear ipv6 mroute statistics

Overview Use this command to delete multicast route statistics entries from the IPv6 multicast routing table.

NOTE: *Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the clear ipv6 mroute command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous static IPv6 multicast routes.*

Syntax

```
clear ipv6 mroute statistics {*|<ipv6-group-address>
[<ipv6-source-address>]}
```

Parameter	Description
*	All multicast route entries.
<ipv6-group-addr>	Group IPv6 address, in hexadecimal notation in the format X.X::X.X.
<ipv6-source-addr>	Source IPv6 address, in hexadecimal notation in the format X.X::X.X.

Mode Privileged Exec

Examples

```
awplus# clear ipv6 mroute statistics 2001::2 ff08::1
awplus# clear ipv6 mroute statistics *
```

ipv6 multicast forward-slow-path-packet

Overview Use this command to enable multicast packets to be forwarded to the CPU. Enabling this command will ensure that the layer L3 MTU is set correctly for each IP multicast group and will apply the value of the smallest MTU among the outgoing interfaces for the multicast group.

It will also ensure that a received packet that is larger than the MTU value will result in the generation of an ICMP Too Big message.

Use the **no** variant of this command to disable the above functionality.

Syntax

```
ipv6 multicast forward-slow-path-packet
no ipv6 multicast forward-slow-path-packet
```

Default Disabled.

Mode Privileged Exec

Example To enable the ipv6 multicast forward-slow-path-packet function, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast forward-slow-path-packet
```

Related commands show ipv6 forwarding

debug nsm

Overview This command specifies a set of debug options for use by Allied Telesis authorized service personnel only.

Use the **no** variant of this command to remove debug options.

Syntax

```
debug nsm [all|events|ha|kernel]
no debug nsm [all|events|ha|kernel]
```

Parameter	Description
`all`	Enables all the nsm debugging options
`events`	Enables the nsm events debugging options
`ha`	Enables the nsm high availability debugging options
`kernel`	Enables the nsm kernel debugging options

Mode Global Configuration, Privileged Exec

Usage notes This command is intended for use by Allied Telesis authorized service personnel for diagnostic purposes.

Related commands show debugging nsm mcast

Command changes Version 5.4.7-2.1 command added.

debug nsm mcast

Overview Use this command to debug IPv4 events in the Multicast Routing Information Base (MRIB).

This command is intended for use by Allied Telesis authorized service personnel for diagnostic purposes.

Syntax

```
debug nsm mcast
{all|fib-msg|mrt|mtrace|mtrace-detail|register|stats|vif}
```

Parameter	Description
`all`	All IPv4 multicast debugging.
`fib-msg`	Forwarding Information Base (FIB) messages.
`mrt`	Multicast routes.
`mtrace`	Multicast traceroute.
`mtrace-detail`	Multicast traceroute detailed debugging.
`register`	Multicast PIM register messages.
`stats`	Multicast statistics.
`vif`	Multicast interface.

Mode Privileged Exec and Global Configuration

Examples To enable debugging of all multicast route events, use the commands:

```
awplus# configure terminal
awplus(config)# debug nsm mcast all
```

To enable debugging of PIM register entries, use the commands:

```
awplus# configure terminal
awplus(config)# debug nsm mcast register
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

debug nsm mcast6

Overview Use this command to debug IPv6 events in the Multicast Routing Information Base (MRIB).

This command is intended for use by Allied Telesis authorized service personnel for diagnostic purposes.

Syntax

```
debug nsm mcast6 {all|fib-msg|mrt|register|stats|vif}
no debug nsm mcast6 {all|fib-msg|mrt|register|stats|vif}
```

Parameter	Description
`all`	All IPv6 multicast route debugging.
`fib-msg`	Forwarding Information Base (FIB) messages.
`mrt`	Multicast routes.
`register`	Multicast PIM register messages.
`stats`	Multicast statistics.
`vif`	Multicast interfaces.

Mode Privileged Exec and Global Configuration

Examples To enable debugging of all multicast route events, use the commands:

```
awplus# configure terminal
awplus(config)# debug nsm mcast6 all
```

To enable debugging of PIM register entries, use the commands:

```
awplus# configure terminal
awplus(config)# debug nsm mcast6 register
```

ip mroute

Overview Use this command to inform multicast of the RPF (Reverse Path Forwarding) route to a given IPv4 multicast source.

Use the **no** variant of this command to delete a route to an IPv4 multicast source.

Syntax

```
ip mroute <ipv4-source-address/mask-length>
[bgp|ospf|rip|static] <rpf-address> [<admin-distance>]
```

```
no ip mroute <ipv4-source-address/mask-length>
[bgp|ospf|rip|static]
```

Parameter	Description
<ipv4-source-address/mask-length>	A multicast source IPv4 address and mask length, in dotted decimal notation in the format A.B.C.D/M.
`bgp`	BGP unicast routing protocol.
`ospf`	OSPF unicast routing protocol.
`rip`	RIP unicast routing protocol.
`static`	Specifies a static route.
<rpf-address>	A.B.C.D The closest known address on the multicast route back to the specified source. This host IPv4 address can be within a directly connected subnet or within a remote subnet. In the case that the address is in a remote subnet, a lookup is done from the unicast route table to find the next hop address on the path to this host.
<admin-distance>	The administrative distance. Use this to determine whether the RPF lookup selects the unicast or multicast route. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence. The default is 0 and the range available is 0-255.

Mode Global Configuration

Usage notes Typically, when a Layer 3 multicast routing protocol is determining the RPF (Reverse Path Forwarding) interface for the path to an IPv4 multicast source, it uses the unicast route table to find the best path to the source. However, in some networks a deliberate choice is made to send multicast via different paths to those used for unicast. In this case, the interface via which a multicast stream from a given source enters a router may not be the same as the interface that connects to the best unicast route to that source.

This command enables the user to statically configure the device with “multicast routes” back to given sources. When performing the RPF check on a stream from a given IPv4 source, the multicast routing protocol will look at these static entries as well as looking into the unicast routing table. The route with the lowest

administrative distance - whether a static “multicast route” or a route from the unicast route table - will be chosen as the RPF route to the source.

Note that in this context the term “multicast route” does not imply a route via which the current router will forward multicast; instead it refers to the route the multicast will have traversed in order to arrive at the current router.

Examples The following example creates a static multicast IPv4 route back to the sources in the 10.10.3.0/24 subnet. The multicast route is via the host 192.168.2.3, and has an administrative distance of 2:

```
awplus# configure terminal
awplus(config)# ip mroute 10.10.3.0/24 static 2 192.168.2.3 2
```

The following example creates a static multicast IPv4 route back to the sources in the 192.168.3.0/24 subnet. The multicast route is via the host 10.10.10.50. The administrative distance on this route has the default value of 0:

```
awplus# configure terminal
awplus(config)# ip mroute 192.168.3.0/24 10.10.10.50
```

Validation Commands show ip rpf

ip multicast allow-register-fragments

Overview Use this command to allow PIM to register fragmented packets. It is disabled by default.

Use the **no** variant of this command to stop PIM from registering fragmented packets.

Syntax

```
ip multicast allow-register-fragments
no ip multicast allow-register-fragments
```

Default This command is disabled by default

Mode Global Configuration

Usage notes Most multicast streams are not fragmented, and therefore this command is unnecessary. By default, when IP multicast packets are fragmented, the switch attempts to reassemble them before registering the packets. This is necessary for tasks such as network address translation, or a firewall.

However, reassembly may be difficult for switches where the CPU cannot handle a large amount of traffic. In that situation, with the CPU failing to reassemble the fragmented packets, there can be a delay in forwarding multicast streams.

We do not recommend enabling this feature if a firewall or network address translation is being used. This feature should only be enabled if multicast data is fragmented and the data rate is too high for the CPU to manage reassembly.

Example To allow PIM to register fragmented packets, use the commands:

```
awplus# configure terminal
awplus(config)# ip multicast allow-register-fragments
```

ip multicast forward-first-packet

Overview Use this command to enable multicast to forward the first multicast packets coming to the device.

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

Syntax

```
ip multicast forward-first-packet
no ip multicast forward-first-packet
```

Default By default, this feature is disabled.

Mode Global Configuration

Usage notes If this command is enabled, the device will forward the first packets in a multicast stream that create the multicast route, possibly causing degradation in the quality of the multicast stream, such as the pixelation of video and audio data.

NOTE: *If you use this command, ensure that the ip igmp snooping command is enabled, the default setting, otherwise the device will not process the first packets of the multicast stream correctly.*

The device will forward the first multicast packets to all interfaces which are on the same VLAN as those which asked for this multicast group.

Examples To enable the forwarding of the first multicast packets, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast forward-first-packet
```

To disable the forwarding of the first multicast packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast forward-first-packet
```

ip multicast route

Overview Use this command to add an IPv4 static multicast route for a specific multicast source and group IPv4 address to the multicast Routing Information Base (RIB). This IPv4 multicast route is used to forward multicast traffic from a specific source and group ingressing on an upstream VLAN to a single or range of downstream VLANs.

Use the **no** variant of this command to either remove an IPv4 static multicast route set with this command or to remove a specific downstream VLAN interface from an IPv4 static multicast route for a specific multicast source and group IPv4 address.

Syntax

```
ip multicast route <ipv4-source-addr> <ipv4-group-addr>
<upstream-vlan-id> [<downstream-vlan-id>]

no ip multicast route <ipv4-source-addr> <ipv4-group-addr>
[<upstream-vlan-id> <downstream-vlan-id>]
```

Parameter	Description
<ipv4-source-addr>	Source IPv4 address, in dotted decimal notation in the format A.B.C.D.
<ipv4-group-addr>	Group IPv4 address, in dotted decimal notation in the format A.B.C.D.
<upstream-vlan-id>	Upstream VLAN interface on which the multicast packets ingress.
<downstream-vlan-id>	Downstream VLAN interface or range of VLAN interfaces to which the multicast packets are sent.

Default By default, this feature is disabled.

Mode Global Configuration

Usage notes Only one multicast route entry per IPv4 address and multicast group can be specified. Therefore, if one entry for a static multicast route is configured, PIM will not be able to update this multicast route in any way.

If a dynamic multicast route exists you cannot create a static multicast route with same source IPv4 address, group IPv4 address, upstream VLAN and downstream VLANs. An error message is displayed and logged. To add a new static multicast route, either wait for the dynamic multicast route to timeout or clear the dynamic multicast route with the clear ip mroute command.

To update an existing static multicast route entry with more or a new set of downstream VLANs, you must firstly remove the existing static multicast route and then add the new static multicast route with all downstream VLANs specified. If you attempt to update an existing static multicast route entry with an additional VLAN or VLANs an error message is displayed and logged.

To create a blackhole or null route where packets from a specified source and group address coming from an upstream VLAN are dropped rather than

forwarded, do not specify the optional <*downstream-vlan-id*> parameter when entering this command.

To remove a specific downstream VLAN from an existing static multicast route entry, specify the VLAN you want to remove with the `<downstream-vlan-id>` parameter when entering the **no** variant of this command.

Examples To create a static multicast route for the multicast source IPv4 address `2.2.2.2` and group IPv4 address `224.9.10.11`, specifying the upstream VLAN interface as `vlan10` and the downstream VLAN interface as `vlan20`, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11 vlan10
vlan20
```

To create a blackhole route for the multicast source IPv4 address `2.2.2.2` and group IPv4 address `224.9.10.11`, specifying the upstream VLAN interface as `vlan10`, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11 vlan10
```

To create an IPv4 static multicast route for the multicast source IPv4 address `2.2.2.2` and group IP address `224.9.10.11`, specifying the upstream VLAN interface as `vlan10` and the downstream VLAN range as `vlan20-25`, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11 vlan10
vlan20-25
```

To remove the downstream VLAN `23` from the IPv4 static multicast route created with the above command, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast route 2.2.2.2 224.9.10.11
vlan10 vlan23
```

To delete an IPv4 static multicast route for the multicast source IP address `2.2.2.2` and group IP address `224.9.10.11`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast route 2.2.2.2 224.9.10.11
```

Related commands clear ip mroute

show ip mroute

ip multicast route-limit

Overview Use this command to limit the number of multicast routes that can be added to an IPv4 multicast routing table.

Use the **no** variant of this command to return the IPv4 route limit to the default.

Syntax

```
ip multicast route-limit <limit> [<threshold>]
no ip multicast route-limit
```

Parameter	Description
<limit>	*<1-2147483647>* Number of routes.
<threshold>	*<1-2147483647>* Threshold above which to generate a warning message. The mroute warning threshold must not exceed the mroute limit.

Default The default limit and threshold value is 2147483647.

Mode Global Configuration

Usage notes This command limits the number of multicast IPv4 routes (mroutes) that can be added to a router, and generates an error message when the limit is exceeded. If the threshold parameter is set, a threshold warning message is generated when this threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the limit argument.

Examples

```
awplus# configure terminal
awplus(config)# ip multicast route-limit 34 24
awplus# configure terminal
awplus(config)# no ip multicast route-limit
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip multicast wrong-vif-suppression

Overview Use this command to prevent unwanted multicast packets received on an unexpected VLAN being trapped to the CPU.

Use the no variant of this command to disable wrong VIF suppression.

Syntax

```
ip ip multicast wrong-vif-suppression
no ip multicast wrong-vif-suppression
```

Default By default, this feature is disabled.

Mode Global Configuration

Usage notes Use this command if there is excessive CPU load and multicast traffic is enabled. To confirm that VIF messages are being sent to the CPU use the debug nsm mcast6 command.

Examples To enable the suppression of wrong VIF packets, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast wrong-vif-suppression
```

To disable the suppression of wrong VIF packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast wrong-vif-suppression
```

ip multicast-routing

Overview Use this command to turn on/off IPv4 multicast routing on the router; when turned off the device does not perform multicast functions.

Use the **no** variant of this command to disable IPv4 multicast routing after enabling it. Note the default stated below.

Syntax

```
ip multicast-routing
no ip multicast-routing
```

Default By default, IPv4 multicast routing is off.

Mode Global Configuration

Usage notes When the **no** variant of this command is used, the Multicast Routing Information Base (MRIB) cleans up Multicast Routing Tables (MRT), stops IGMP operation, and stops relaying multicast forwarder events to multicast protocols.

When multicast routing is enabled, the MRIB starts processing any MRT addition/deletion requests, and any multicast forwarding events.

You must enable multicast routing before issuing other multicast commands.

Example

```
awplus# configure terminal
awplus(config)# ip multicast-routing
```

Validation Commands show running-config

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ipv6 mroute

Overview Use this command to inform multicast of the RPF (Reverse Path Forwarding) route to a given IPv6 multicast source.

Use the **no** variant of this command to delete a route to an IPv6 multicast source.

Syntax

```
ipv6 mroute <ipv6-source-address/mask-length> [rip|static]
<rpf-address> [<admin-distance>]
no ipv6 mroute <ipv6-source-address/mask-length> [rip|static]
```

Parameter	Description
<ipv6-source-address/mask-length>	A multicast source IPv6 address and mask length, in hexadecimal notation in the format X.X::X.X/M.
`rip`	RIPng IPv6 unicast routing protocol.
`static`	Specifies a static route.
<rpf-address>	X.X::X:X The closest known address on the IPv6 multicast route back to the specified source. This host IPv6 address can be within a directly connected subnet or within a remote subnet. In the case that the address is in a remote subnet, a lookup is done from the unicast route table to find the nexthop address on the path to this host.
<admin-distance>	The administrative distance. Use this to determine whether the RPF lookup selects the unicast or multicast route. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence. The default is `0` and the range available is `0-255`.

Mode Global Configuration

Usage notes Typically, when a Layer 3 multicast routing protocol is determining the RPF (Reverse Path Forwarding) interface for the path to a multicast source, it uses the unicast IPv6 route table to find the best path to the source. However, in some networks a deliberate choice is made to send multicast via different paths to those used for unicast. In this case, the interface via which a multicast stream from a given source enters a router may not be the same as the interface that connects to the best unicast route to that source.

This command enables the user to statically configure the switch with “multicast routes” back to given sources. When performing the RPF check on a stream from a given IPv6 source, the multicast routing protocol will look at these static entries as well as looking into the unicast routing table. The route with the lowest administrative distance - whether a static “multicast route” or a route from the unicast route table - will be chosen as the RPF route to the source.

Note that in this context the term “multicast route” does not imply a route via which the current router will forward multicast; instead it refers to the route the multicast will have traversed in order to arrive at the current router.

Examples

The following example creates a static multicast route back to the sources in the `2001::1/64` subnet. The multicast route is via the host `2002::2`, and has an administrative distance of `2`:

```
awplus# configure terminal
awplus(config)# ipv6 mroute 2001::1/64 static 2 2002::2
```

The following example creates a static multicast route back to the sources in the 2002::2/64subnet. The multicast route is via the host 2001::1. The administrative distance on this route has the default value of `0`:

```
awplus# configure terminal
awplus(config)# ipv6 mroute 2002::2/64 2001::1
```

Validation Commands

show ipv6 mroute

ipv6 multicast route

Overview Use this command to add an IPv6 static multicast route for a specific multicast source and group IPv6 address to the multicast Routing Information Base (RIB). This IPv6 multicast route is used to forward IPv6 multicast traffic from a specific source and group ingressing on an upstream VLAN to a single or range of downstream VLANs.

See detailed usage notes below to configure static multicast router ports when using static IPv6 multicast routes with EPSR, and the destination VLAN is an EPSR data VLAN.

Use the **no** variant of this command to either remove an IPv6 static multicast route set with this command or to remove a specific downstream VLAN interface from an IPv6 static multicast route for a specific IPv6 multicast source and group address.

Syntax

```
ipv6 multicast route <ipv6-source-addr> <ipv6-group-addr>
<upstream-vlan-id> [<downstream-vlan-id>]
```

```
no ipv6 multicast route <ipv6-source-addr> <ipv6-group-addr>
[<upstream-vlan-id> <downstream-vlan-id>]
```

Parameter	Description
<ipv6-group-addr>	Source IPv6 address, in dotted decimal notation in the format X.X::X.X.
<ipv6-group-addr>	Group IP address, in dotted decimal notation in the format X.X::X.X.
<upstream-vlan-id>	Upstream VLAN interface on which the multicast packets ingress.
<downstream-vlan-id>	Downstream VLAN interface or range of VLAN interfaces to which the multicast packets are sent.

Default By default, no static routes exist.

Mode Global Configuration

Usage notes Only one multicast route entry per IPv6 address and multicast group can be specified. Therefore, if one entry for an IPv6 static multicast route is configured, PIM will not be able to update this multicast route in any way.

If a dynamic multicast route exists, you cannot create a static multicast route with the same source IPv6 address and group IPv6 address. An error message is displayed and logged. To add a new static multicast route, either wait for the dynamic multicast route to time out or clear the dynamic multicast route with the clear ipv6 mroute command.

To update an existing IPv6 static multicast route entry with new or additional downstream VLANs, you must firstly remove the existing static multicast route and then add the new static multicast route with all downstream VLANs specified. If

you attempt to update an existing static multicast route entry with an additional VLAN or VLANs an error message is displayed and logged.

To create a blackhole or null route where packets from a specified source and group address coming from an upstream VLAN are dropped rather than forwarded, do not specify the optional <*downstream-vlan-id*> parameter when entering this command.

To remove a specific downstream VLAN from an existing static multicast route entry, specify the VLAN you want to remove with the `<downstream-vlan-id>` parameter when entering the **no** variant of this command.

Note that if static IPv6 multicast routing is being used with EPSR and the destination VLAN is an EPSR data VLAN, then multicast router (mrouter) ports must be statically configured. This minimizes disruption for multicast traffic in the event of ring failure or restoration.

When configuring the EPSR data VLAN, statically configure mrouter ports so that the multicast router can be reached in either direction around the EPSR ring.

For example, if port1.0.1 and port1.0.14 are ports on an EPSR data VLAN vlan101, which is the destination for a static IPv6 multicast route, then configure both ports as multicast router (mrouter) ports as shown in the example commands listed below:

Figure 34-1: Example ipv6 mld snooping mrouter commands when static IPv6 multicast routing is being used and the destination VLAN is an EPSR data VLAN:

```
awplus>enable

awplus#configure terminal

awplus(config)#interface vlan101

awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.1

awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.14
```

See ipv6 mld snooping mrouter for a command description and command examples.

Examples To create an IPv6 static multicast route for the multicast source IPv6 address `2001::1` and group IPv6 address `ff08::1`, specifying the upstream VLAN interface as `vlan10` and the downstream VLAN interface as `vlan20`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 multicast route 2001::1 ff08::1 vlan10
vlan20
```

To create a blackhole route for the IPv6 multicast source IP address 2001::1 and group IP address ff08::1, specifying the upstream VLAN interface as `vlan10`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 multicast route 2001::1 ff08::1 vlan10
```

To create an IPv6 static multicast route for the multicast source IPv6 address 2001::1 and group IPv6 address ff08::1, specifying the upstream VLAN interface as `vlan10` and the downstream VLAN range as `vlan20-25`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 multicast route 2001::1 ff08::1 vlan10
vlan20-25
```

To remove the downstream VLAN `23` from the IPv6 static multicast route created with the above command, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 multicast route 2001::1 ff08::1 vlan10
vlan23
```

To delete an IPv6 static multicast route for the multicast source IPv6 address 2001::1 and group IPv6 address ff08::1, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 multicast route 2001::1 ff08::1
```

Related commands

clear ipv6 mroute

ipv6 mld snooping mrouter

show ipv6 mroute

ipv6 multicast route-limit

Overview Use this command to limit the number of multicast routes that can be added to an IPv6 multicast routing table.

Use the no variant of this command to return the IPv6 route limit to the default.

Syntax

```
ipv6 multicast route-limit <limit> [<threshold>]
no ipv6 multicast route-limit
```

Parameter	Description
<limit>	*<1-2147483647>* Number of routes.
<threshold>	*<1-2147483647>* Threshold above which to generate a warning message. The mroute warning threshold must not exceed the mroute limit.

Default The default limit and threshold value is 2147483647.

Mode Global Configuration

Usage notes This command limits the number of multicast IPv6 routes (mroutes) that can be added to a router, and generates an error message when the limit is exceeded. If the threshold parameter is set, a threshold warning message is generated when this threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the limit argument.

Examples

```
awplus# configure terminal
awplus(config)# ipv6 multicast route-limit 34 24
awplus# configure terminal
awplus(config)# no ipv6 multicast route-limit
```

ipv6 multicast-routing

Overview Use this command to turn on/off IPv6 multicast routing on the router; when turned off the device does not perform multicast functions.

Use the **no** variant of this command to disable IPv6 multicast routing after enabling it. Note the default stated below.

Syntax

```
ipv6 multicast-routing
no ipv6 multicast-routing
```

Default By default, IPv6 multicast routing is off.

Mode Global Configuration

Usage When the **no** variant of this command is used, the Multicast Routing Information Base (MRIB) cleans up Multicast Routing Tables (MRT, and stops relaying multicast forwarder events to multicast protocols.

When multicast routing is enabled, the MRIB starts processing any MRT addition/deletion requests, and any multicast forwarding events.

You must enable multicast routing before issuing other multicast commands.

Examples

```
awplus# configure terminal
awplus(config)# ipv6 multicast-routing
awplus# configure terminal
awplus(config)# no ipv6 multicast-routing
```

Validation Commands show running-config

multicast

Overview Use this command to enable a device port to route multicast packets that ingress the port.

Use the **no** variant of this command to stop the device port from routing multicast packets that ingress the port. Note that this does not affect Layer 2 forwarding of multicast packets. If you enter **no multicast** on a port, multicast packets received on that port will not be forwarded to other VLANs, but ports in the same VLANs as the receiving port will still receive the multicast packets.

CAUTION: *We do not recommend disabling multicast routing in a live network. Some non-multicast protocols use multicast packets and will not function correctly if you disable it.*

Syntax

```
multicast
no multicast
```

Default By default, all device ports route multicast packets.

Mode Interface Configuration

Examples To disable routing of multicast packets on a port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no multicast
```

To re-enable routing of multicast packets on a port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# multicast
```

Validation Commands show running-config

platform multicast-ratelimit

Overview Use this command to set the maximum number of multicast packets to be forwarded to the CPU (in packets per second). Setting the value to zero disables rate limiting.

This command should be used with care. Increasing or removing the limit could make the device less responsive under heavy multicast load.

Use the **no** variant of this command to return the limit to its default.

Syntax

```
platform multicast-ratelimit <0-1000>
no platform multicast-ratelimit
```

Default 10 packets per second (pps)

Mode Global Configuration

Usage notes If you find that the CPU load on your device from multicast traffic is higher than desired, reducing this rate may reduce the CPU load.

If you need the device to process a large amount of multicast traffic, increasing this rate may improve performance.

Example To set the rate to 30pps, use the commands:

```
awplus# configure terminal
awplus(config)# platform multicast-ratelimit 30
```

Command changes Version 5.4.8-1.1: default changed to 100pps on SBx908 GEN2, SBx8100, and x930 Series switches.

show debugging nsm mcast

Overview Use this command to show the status of the NSM multicast debugging.

Syntax

```
show debugging nsm mcast
```

Mode Privileged Exec

Usage notes This command is intended for use by Allied Telesis authorized service personnel for diagnostic purposes.

Example To show debugging for NSM multicast, use the following command:

```
awplus# show debug nsm mcast
```

Output Figure 34-2: Example output from **show debug nsm mcast**

```
awplus# show debugging nsm mcast
Debugging status:
  NSM multicast vif debugging is on
  NSM multicast route debugging is on
  NSM multicast route statistics debugging is on
  NSM multicast FIB message debugging is on
  NSM multicast PIM Register message debugging is on
  NSM multicast traceroute debugging is on
  NSM multicast traceroute detailed debugging is on
```

Related commands debug nsm mcast

Command changes Version 5.4.7-2.1: command added

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2

show ip mroute

Overview Use this command to display the contents of the IPv4 multicast routing (mroute) table.

Syntax
```
show ip mroute [<ipv4-group-addr>] [<ipv4-source-addr>]
[dense|sparse] [count|summary]
```

Parameter	Description
<ipv4-group-addr>	Group IPv4 address, in dotted decimal notation in the format A.B.C.D.
<ipv4-source-addr>	Source IPv4 address, in dotted decimal notation in the format A.B.C.D.
`dense`	Display dense IPv4 multicast routes.
`sparse`	Display sparse IPv4 multicast routes.
`count`	Display the route and packet count from the IPv4 multicast routing (mroute) table.
`summary`	Display the contents of the IPv4 multicast routing (mroute) table in an abbreviated form.

Mode User Exec and Privileged Exec

Examples
```
awplus# show ip mroute 10.10.3.34 224.1.4.3
awplus# show ip mroute 10.10.5.24 225.2.2.2 count
awplus# show ip mroute 10.10.1.34 summary
```

Output The following is a sample output of this command displaying the IPv4 multicast routing table, with and without specifying the group and source IPv4 address:

Figure 34-3: Example output from the **show ip mroute** command

```
awplus# show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SM, Flags: TF
  Incoming interface: vlan2
  Outgoing interface list:
   vlan3 (1)
```

Figure 34-4: Example output from the **show ip mroute** command with the source and group IPv4 address specified

```
awplus# show ip mroute 10.10.1.52 224.0.1.3

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), uptime 00:03:24, stat expires 00:01:28
Owner PIM-SM, Flags: TF
  Incoming interface: vlan2
  Outgoing interface list:
    vlan3 (1)
```

The following is a sample output of this command displaying the packet count from the IPv4 multicast routing table:

Figure 34-5: Example output from the **show ip mroute count** command

```
awplus# show ip mroute count
IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:10

Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If
pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent

(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
  Fwd msg: 0/0, Client msg: 0/0/0/0,  Reg: 0/0/0
```

The following is a sample output for this command displaying the IPv4 multicast routing table in an abbreviated form:

Figure 34-6: Example output from the **show ip mroute summary** command

```
awplus# show ip mroute summary

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM, Flags: TF
```

Command changes

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip mvif

Overview Use this command to display the contents of the IPv4 Multicast Routing Information Base (MRIB) VIF table.

Syntax `show ip mvif <interface>`

Parameter	Description
<interface>	The interface to display information about.

Mode User Exec and Privileged Exec

Example `awplus# show ip mvif vlan2`

Output Figure 34-7: Example output from the **show ip mvif** command

```
Interface     Vif   Owner     TTL  Local             Remote          Uptime
              Idx   Module         Address           Address
vlan2         0     PIM-SM    1    192.168.1.53      0.0.0.0         00:04:26
Register      1               1    192.168.1.53      0.0.0.0         00:04:26
vlan3         2     PIM-SM    1    192.168.10.53     0.0.0.0         00:04:25
```

Figure 34-8: Example output from the **show ip mvif** command with the interface parameter **vlan2** specified

```
Interface     Vif   Owner     TTL  Local             Remote            Uptime
              Idx   Module         Address           Address
vlan2         0     PIM-SM    1    192.168.1.53      0.0.0.0           00:05:17
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip rpf

Overview Use this command to display Reverse Path Forwarding (RPF) information for the specified IPv4 source address.

Syntax

```
show ip rpf <source-addr>
```

Parameter	Description
<source-addr>	Source IPv4 address, in dotted decimal notation in the format A.B.C.D.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip rpf 10.10.10.50
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ipv6 mroute

Overview Use this command to display the contents of the IPv6 multicast routing (mroute) table.

Syntax
```
show ipv6 mroute [<ipv6-group-addr>] [<ipv6-source-addr>]
[{count|summary}]
```

Parameter	Description
<ipv6-group-addr>	Group IPv6 address, in hexadecimal notation in the format X.X::X.X.
<ipv6-source-addr>	Source IPv6 address, in hexadecimal notation in the format X.X::X.X.
`count`	Display the route and packet count from the IPv6 multicast routing (mroute) table.
`summary`	Display the contents of the IPv6 multicast routing (mroute) table in an abbreviated form.

Mode User Exec and Privileged Exec

Examples
```
awplus# show ipv6 mroute
awplus# show ipv6 mroute count
awplus# show ipv6 mroute summary
awplus# show ipv6 mroute 2001::2 ff08::1 count
awplus# show ipv6 mroute 2001::2 ff08::1
awplus# show ipv6 mroute 2001::2 summary
```

Output The following is a sample output of this command displaying the IPv6 multicast routing table for a single static IPv6 Multicast route:

Figure 34-9: Example output from the **show ipv6 mroute** command

```
awplus#show ipv6 mroute
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface
(2001::2, ff08::1), uptime 03:18:38
Owner IMI, Flags: F
  Incoming interface: vlan2
  Outgoing interface list:
    vlan3
```

The following is a sample output of this command displaying the IPv6 multicast routing count table for a single static IPv6 Multicast route:

Figure 34-10: Example output from the **show ipv6 mroute count** command

```
awplus#show ipv6 mroute count

IPv6 Multicast Statistics
Total 1 routes using 152 bytes memory
Route limit/Route threshold: 1024/1024
Total NOCACHE/WRONGmif/WHOLEPKT recv from fwd: 6/0/0
Total NOCACHE/WRONGmif/WHOLEPKT sent to clients: 6/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:14

Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If
pkts
Fwd msg counts: WRONGmif/WHOLEPKT recv
Client msg counts: WRONGmif/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent

(2001::2, ff08::1), Forwarding: 0/0, Other: 0
  Fwd msg: 0/0, Client msg: 0/0/0/0,  Reg: 0/0/0
```

The following is a sample output of this command displaying the IPv6 multicast routing summary table for a single static IPv6 Multicast route:

Figure 34-11: Example output from the **show ipv6 mroute summary** command

```
awplus#show ipv6 mroute summary
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface

(2001::2, ff08::1), 03:20:28/-, IMI, Flags: F
```

show ipv6 multicast forwarding

Overview Use this command to view the status of multicast forwarding slow-path-packet setting.

Syntax

```
show ipv6 multicast forwarding
```

Mode User Exec

Example To show the status of the multicast forwarding, slow-path-packet setting, use the following command:

```
awplus# show ipv6 multicast forwarding
```

Output Figure 34-12: Example output from the **show ipv6 multicast forwarding** command:

```
ipv6 multicast forwarding is disabled
```

Related commands ipv6 multicast forward-slow-path-packet

show ipv6 mif

Overview Use this command to display the contents of the IPv6 Multicast Routing Information Base (MRIB) MIF table.

Syntax

```
show ipv6 mif [<interface>]
```

Parameter	Description
<interface>	The interface to display information about.

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 mif
awplus# show ipv6 mif vlan2
```

Output Figure 34-13: Example output from the **show ipv6 mif** command

```
awplus#show ipv6 mif
Interface    Mif   Owner             Uptime
             Idx   Module
vlan3        0     MLD/MLD Proxy-Service 03:28:48
vlan2        1     MLD/MLD Proxy-Service 03:28:48
vlan1        2     MLD/MLD Proxy-Service 03:28:48
```

Figure 34-14: Example output from the **show ipv6 mif** command with the interface parameter **vlan2** specified

```
Interface    Mif   Owner     TTL   Remote            Uptime
             Idx   Module          Address
vlan2        0     PIM-SMv6    1     0.0.0.0         00:05:17
```

35 PIM-SM Commands

Introduction

Overview This chapter provides an alphabetical reference of PIM-SM commands. For commands common to PIM-SM and PIM-DM, see the Multicast Commands chapter.

Command List

- "clear ip pim sparse-mode bsr rp-set *" on page 1755
- "clear ip pim sparse-mode packet statistics" on page 1756
- "clear ip mroute pim sparse-mode" on page 1757
- "debug pim sparse-mode" on page 1758
- "debug pim sparse-mode timer" on page 1759
- "ip multicast allow-register-fragments" on page 1761
- "ip pim accept-register list" on page 1762
- "ip pim anycast-rp" on page 1763
- "ip pim bsr-border" on page 1764
- "ip pim bsr-candidate" on page 1765
- "ip pim cisco-register-checksum" on page 1766
- "ip pim cisco-register-checksum group-list" on page 1767
- "ip pim crp-cisco-prefix" on page 1768
- "ip pim dr-priority" on page 1769
- "ip pim exclude-genid" on page 1770
- "ip pim ext-srcs-directly-connected" on page 1771
- "ip pim hello-holdtime (PIM-SM)" on page 1772
- "ip pim hello-interval (PIM-SM)" on page 1773
- "ip pim ignore-rp-set-priority" on page 1774

- "ip pim jp-timer" on page 1775
- "ip pim neighbor-filter (PIM-SM)" on page 1776
- "ip pim register-rate-limit" on page 1777
- "ip pim register-rp-reachability" on page 1778
- "ip pim register-source" on page 1779
- "ip pim register-suppression" on page 1780
- "ip pim rp-address" on page 1781
- "ip pim rp-candidate" on page 1783
- "ip pim rp-register-kat" on page 1785
- "ip pim sparse-mode" on page 1786
- "ip pim sparse-mode join-prune-batching" on page 1787
- "ip pim sparse-mode passive" on page 1788
- "ip pim sparse-mode wrong-vif-suppression" on page 1789
- "ip pim spt-threshold" on page 1790
- "ip pim spt-threshold group-list" on page 1791
- "ip pim ssm" on page 1792
- "service pim" on page 1793
- "show debugging pim sparse-mode" on page 1794
- "show ip pim sparse-mode bsr-router" on page 1795
- "show ip pim sparse-mode interface" on page 1796
- "show ip pim sparse-mode interface detail" on page 1798
- "show ip pim sparse-mode local-members" on page 1799
- "show ip pim sparse-mode mroute" on page 1800
- "show ip pim sparse-mode mroute detail" on page 1802
- "show ip pim sparse-mode neighbor" on page 1804
- "show ip pim sparse-mode nexthop" on page 1805
- "show ip pim sparse-mode packet statistics" on page 1806
- "show ip pim sparse-mode rp-hash" on page 1807
- "show ip pim sparse-mode rp mapping" on page 1808
- "undebug all pim sparse-mode" on page 1809

clear ip pim sparse-mode bsr rp-set *

Overview Use this command to clear all Rendezvous Point (RP) sets learned through the PIMv2 Bootstrap Router (BSR).

Syntax

```
clear ip pim sparse-mode bsr rp-set *
```

Parameter	Description
*	Clears all RP sets.

Mode Privileged Exec

Usage notes For multicast clients, note that one router will be automatically or statically designated as the RP, and all routers must explicitly join through the RP. A Designated Router (DR) sends periodic Join/Prune messages toward a group-specific RP for each group that it has active members.

For multicast sources, note that the Designated Router (DR) unicasts Register messages to the RP encapsulating the data packets from the multicast source. The RP forwards decapsulated data packets toward group members.

Example

```
awplus# clear ip pim sparse-mode bsr rp-set *
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

clear ip pim sparse-mode packet statistics

Overview Use this command to clear the PIM sparse mode packet statistics counter.

Syntax
```
clear ip pim sparse-mode packet statistics
```

Mode Privileged Exec

Example The following command clears the current packet receive counts for PIM sparse-mode:

```
awplus# configure terminal
awplus(config)# clear ip pim sparse-mode statistics
```

Output Figure 35-1: Example output from **clear ip pim sparse-mode statistics**

```
awplus(config)#clear ip pim sparse-mode statistics
PIM-SM Receive Packet Statistics :
All PIM-SM    :   Total : 0   Valid : 0
Hello         :   Total : 0   Valid : 0
Register      :   Total : 0   Valid : 0
Register Stop :   Total : 0   Valid : 0
Join/Prune    :   Total : 0   Valid : 0
Bootstrap     :   Total : 0   Valid : 0
Assert        :   Total : 0   Valid : 0
Candidate-RP  :   Total : 0   Valid : 0
```

Related commands show ip pim sparse-mode packet statistics

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

clear ip mroute pim sparse-mode

Overview Use this command to clear all multicast route table entries learned through PIM-SM for a specified multicast group address, and optionally a specified multicast source address.

Syntax

```
clear ip mroute <Group-IP-address> pim sparse-mode
clear ip mroute <Group-IP-address> <Source-IP-address> pim sparse-mode
```

Parameter	Description
<Group-IP-address>	Specify a multicast group IPv6 address, entered in the form A.B.C.D.
<Source-IP-address>	Specify a source group IP address, entered in the form A.B.C.D.

Mode Privileged Exec

Example

```
awplus# clear ip mroute  pim sparse-mode 224.0.0.0
awplus# clear ip mroute  192.168.7.1 pim sparse-mode 224.0.0.0
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

debug pim sparse-mode

Overview Use this command to turn on some or all PIM-SM debugging.

Use the **no** variant of this command to turn off some or all PIM-SM debugging.

Syntax

```
debug pim sparse-mode [all] [events] [mfc] [mib] [nexthop] [nsm]
[packet] [state] [mtrace]
```

```
no debug pim sparse-mode [all] [events] [mfc] [mib] [nexthop]
[nsm] [packet] [state] [mtrace]
```

Parameter	Description
`all`	Activates/deactivates all PIM-SM debugging.
`events`	Activates debug printing of events.
`mfc`	Activates debug printing of MFC (Multicast Forwarding Cache in kernel) add/delete/updates.
`mib`	Activates debug printing of PIM-SM MIBs.
`nexthop`	Activates debug printing of PIM-SM next hop communications.
`nsm`	Activates debugging of PIM-SM Network Services Module communications.
`packet`	Activates debug printing of incoming and/or outgoing packets.
`state`	Activates debug printing of state transition on all PIM-SM FSMs.
`mtrace`	Activates debug printing of multicast traceroute.

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# debug pim sparse-mode all
```

Related commands show debugging pim sparse-mode

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

debug pim sparse-mode timer

Overview Use this command to enable debugging for the specified PIM-SM timers.

Use the **no** variants of this command to disable debugging for the specified PIM-SM timers.

Syntax

```
debug pim sparse-mode timer assert [at]
no debug pim sparse-mode timer assert [at]
debug pim sparse-mode timer bsr [bst|crp]
no debug pim sparse-mode timer bsr [bst|crp]
debug pim sparse-mode timer hello [ht|nlt|tht]
no debug pim sparse-mode timer hello [ht|nlt|tht]
debug pim sparse-mode timer joinprune [jt|et|ppt|kat|ot]
no debug pim sparse-mode timer joinprune [jt|et|ppt|kat|ot]
debug pim sparse-mode timer register [rst]
no debug pim sparse-mode timer register [rst]
```

Parameter	Description
`assert`	Enable or disable debugging for the Assert timers.
`at`	Enable or disable debugging for the Assert Timer.
`bsr`	Enable or disable debugging for the specified Bootstrap Router timer, or all Bootstrap Router timers.
`bst`	Enable or disable debugging for the Bootstrap Router: Bootstrap Timer.
`crp`	Enable or disable debugging for the Bootstrap Router: Candidate-RP Timer.
`hello`	Enable or disable debugging for the specified Hello timer, or all Hello timers.
`ht`	Enable or disable debugging for the Hello timer: Hello Timer.
`nlt`	Enable or disable debugging for the Hello timer: Neighbor Liveness Timer.
`tht`	Enable or disable debugging for the Hello timer: Triggered Hello Timer.
`joinprune`	Enable or disable debugging for the specified JoinPrune timer, or all JoinPrune timers.
`jt`	Enable or disable debugging for the JoinPrune timer: upstream Join Timer.
`et`	Enable or disable debugging for the JoinPrune timer: Expiry Timer.
`ppt`	Enable or disable debugging for the JoinPrune timer: PrunePending Timer.

Parameter	Description
`kat`	Enable or disable debugging for the JoinPrune timer: KeepAlive Timer.
`ot`	Enable or disable debugging for the JoinPrune timer: Upstream Override Timer.
`register`	Enable or disable debugging for the Register timers.
`rst`	Enable or disable debugging for the Register timer: Register Stop Timer.

Default By default, all debugging is disabled.

Mode Privileged Exec and Global Configuration

Examples To enable debugging for the PIM-SM Bootstrap Router bootstrap timer, use the commands:

```
awplus(config)# debug pim sparse-mode timer bsr bst
```

To enable debugging for the PIM-SM Hello: neighbor liveness timer, use the command:

```
awplus(config)# debug pim sparse-mode timer hello ht
```

To enable debugging for the PIM-SM Joinprune expiry timer, use the command:

```
awplus# debug pim sparse-mode timer joinprune et
```

To disable debugging for the PIM-SM Register timer, use the command:

```
awplus# no debug pim sparse-mode timer register
```

Related commands show debugging pim sparse-mode

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip multicast allow-register-fragments

Overview Use this command to allow PIM to register fragmented packets. It is disabled by default.

Use the **no** variant of this command to stop PIM from registering fragmented packets.

Syntax

```
ip multicast allow-register-fragments
no ip multicast allow-register-fragments
```

Default This command is disabled by default

Mode Global Configuration

Usage notes Most multicast streams are not fragmented, and therefore this command is unnecessary. By default, when IP multicast packets are fragmented, the switch attempts to reassemble them before registering the packets. This is necessary for tasks such as network address translation, or a firewall.

However, reassembly may be difficult for switches where the CPU cannot handle a large amount of traffic. In that situation, with the CPU failing to reassemble the fragmented packets, there can be a delay in forwarding multicast streams.

We do not recommend enabling this feature if a firewall or network address translation is being used. This feature should only be enabled if multicast data is fragmented and the data rate is too high for the CPU to manage reassembly.

Example To allow PIM to register fragmented packets, use the commands:

```
awplus# configure terminal
awplus(config)# ip multicast allow-register-fragments
```

ip pim accept-register list

Overview Use this command to configure the ability to filter out multicast sources specified by the given access-list at the Rendezvous Point (RP), so that the RP will accept/refuse to perform the register mechanism for the packets sent by the specified sources.

Use the **no** variant of this command to revert to default.

Syntax

```
ip pim accept-register list {<100-199>|<2000-2699>|<name>}
no ip pim accept-register
```

Parameter	Description
<100-199>	IP extended access-list, identified by number.
<2000-2699>	IP extended access list, identified by number (expanded range).
<name>	IP access list, identified by name.

Default By default, the RP accepts register packets from all multicast sources.

Mode Global Configuration

Example To create an ACL that denies packets from 100.1.1.1 to any destination, and use that ACL to filter at the RP point, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 121
awplus(config-ip-ext-acl)# deny ip 100.1.1.1 0.0.0.0 any
awplus(config-ip-ext-acl)# exit
awplus(config)# ip pim accept-register list 121
```

ip pim anycast-rp

Overview Use this command to configure Anycast RP (Rendezvous Point) in a RP set.

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

Syntax

```
ip pim anycast-rp <anycast-rp-address> <member-rp-address>
no ip pim anycast-rp <anycast-rp-address> [<member-rp-address>]
```

Parameter	Description
<anycast-rp-address>	<A.B.C.D> Specify an anycast IP address to configure an Anycast RP (Rendezvous Point) in a RP set.
<member-rp-address>	<A.B.C.D> Specify an Anycast RP (Rendezvous Point) address to configure an Anycast RP in a RP set.

Mode Global Configuration

Usage notes Anycast is a network addressing and routing scheme where data is routed to the nearest or best destination as viewed by the routing topology. Compared to unicast with a one-to- one association between network address and network endpoint, and multicast with a one-to-many association between network address and network endpoint; anycast has a one-to-many association between network address and network endpoint. For anycast, each destination address identifies a set of receiver endpoints, from which only one receiver endpoint is chosen.

Anycast is often implemented using BGP to simultaneously advertise the same destination IP address range from many sources, resulting in packets address to destination addresses in this range being routed to the nearest source announcing the given destination IP address.

Use this command to specify the Anycast RP configuration in the Anycast RP set. Use the **no** variant of this command to remove the Anycast RP configuration. Note that the member RP address is optional when using the **no** parameter to remove the Anycast RP configuration. removing the anycast RP address also removes the member RP address.

Examples The following example shows how to configure the Anycast RP address with **ip pim anycast-rp**:

```
awplus# configure terminal
awplus(config)# ip pim anycast-rp 1.1.1.1 10.10.10.10
```

The following example shows how to remove the Anycast RP in the RP set specifying only the anycast RP address with **no ip pim anycast-rp**, but not specifying the member RP address:

```
awplus# configure terminal
awplus(config)# no ip pim anycast-rp 1.1.1.1
```

ip pim bsr-border

Overview Use the **ip pim bsr-border** command to prevent Bootstrap Router (BSR) messages from being sent or received through a VLAN interface. The BSR border is the border of the PIM domain.

Use the **no** variant of this command to disable the configuration set with **ip pim bsr-border**.

Syntax

```
ip pim bsr-border
no ip pim bsr-border
```

Mode Interface Configuration for a VLAN interface.

Usage notes When this command is configured on a VLAN interface, no PIM version 2 BSR messages will be sent or received through the interface. Configure an interface bordering another PIM domain with this command to avoid BSR messages from being exchanged between the two PIM domains.

BSR messages should not be exchanged between different domains, because devices in one domain may elect Rendezvous Points (RPs) in the other domain, resulting in loss of isolation between the two PIM domains that would stop the PIM protocol from working as intended.

Examples The following example configures the VLAN interface vlan2 to be the PIM domain border:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim bsr-border
```

The following example removes the VLAN interface vlan2 from the PIM domain border:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip pim bsr-border
```

ip pim bsr-candidate

Overview Use this command to give the device the candidate BSR (Bootstrap Router) status using the specified IP address mask of the interface.

Use the **no** variant of this command to withdraw the address of the interface from being offered as a BSR candidate.

Syntax

```
ip pim bsr-candidate <interface> [<hash>] [<priority>]
no ip pim bsr-candidate [<interface>]
```

Parameter	Description
<interface>	The interface. For instance, `vlan2`.
<hash>	<0-32> configure hash mask length for RP selection. The default hash value if you do not configure this parameter is 10.
<priority>	<0-255> configure priority for a BSR candidate. Note that you must also specify the <*hash*> (mask length) when specifying the <*priority*>. The default priority if you do not configure this parameter is 64.

Mode Global Configuration

Default The default hash parameter value is 10 and the default priority parameter value is 64.

Examples To set the BSR candidate to the VLAN interface vlan2, with the optional mask length and BSR priority parameters, enter the commands shown below:

```
awplus# configure terminal
awplus(config)# ip pim bsr-candidate vlan2 20 30
```

To withdraw the address of vlan2 from being offered as a BSR candidate, enter:

```
awplus# configure terminal
awplus(config)# no ip pim bsr-candidate vlan2
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim cisco-register-checksum

Overview Use this command to configure the option to calculate the Register checksum over the whole packet. This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to disable this option.

Syntax
```
ip pim cisco-register-checksum
no ip pim cisco-register-checksum
```

Default This command is disabled by default. By default, Register Checksum is calculated only over the header.

Mode Global Configuration

Example
```
awplus# configure terminal
awplus(config)# ip pim cisco-register-checksum
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim cisco-register-checksum group-list

Overview Use this command to configure the option to calculate the Register checksum over the whole packet on multicast groups specified by the access-list. This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to revert to default settings.

Syntax

```
ip pim cisco-register-checksum group-list <acl>
no ip pim cisco-register-checksum group-list <acl>
```

Parameter	Description
<acl>	The standard, expanded or named ACL to use.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# ip pim cisco-register-checksum group-list 34
awplus(config)# access-list 34 permit 224.0.1.3
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim crp-cisco-prefix

Overview Use this command to interoperate with Cisco devices that conform to an earlier draft standard. Some Cisco devices might not accept candidate RPs with a group prefix number of zero. Note that the latest BSR specification prohibits sending RP advertisements with prefix 0. RP advertisements for the default IPv4 multicast group range 224/4 are sent with a prefix of 1.

Use the **no** variant of this command to revert to the default settings.

Syntax

```
ip pim crp-cisco-prefix
no ip pim crp-cisco-prefix
```

Mode Global Configuration

Usage notes Cisco's BSR code does not conform to the latest BSR draft. It does not accept candidate RPs with a group prefix number of zero. To make the candidate RP work with a Cisco BSR, use the **ip pim crp-cisco-prefix** command when interoperating with older versions of Cisco IOS.

Example

```
awplus# configure terminal
awplus(config)# ip pim crp-cisco-prefix
awplus# configure terminal
awplus(config)# no ip pim crp-cisco-prefix
```

Related commands ip pim rp-candidate

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim dr-priority

Overview Use this command to set the Designated Router priority value.

Use the **no** variant of this command to disable this function.

Syntax

```
ip pim dr-priority  <priority>
no ip pim dr-priority [<priority>]
```

Parameter	Description
<priority>	<0-4294967294> The Designated Router priority value. A higher value has a higher preference.

Default The default is 1. The negated form of this command restores the value to the default.

Mode Interface Configuration for a VLAN interface.

Examples To set the Designated Router priority value to 11234 for the VLAN interface vlan2, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim dr-priority 11234
```

To disable the Designated Router priority value for the VLAN interface vlan2, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip pim dr-priority
```

Related commands ip pim ignore-rp-set-priority

ip pim exclude-genid

Overview Use this command to exclude the GenID option from Hello packets sent out by the PIM module on a particular interface.This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to revert to default settings.

Syntax
```
ip pim exclude-genid
no ip pim exclude-genid
```

Default By default, this command is disabled; the GenID option is included.

Mode Interface Configuration for a VLAN interface.

Example
```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim exclude-genid
```

ip pim ext-srcs-directly-connected

Overview Use this command to configure PIM to treat all source traffic arriving on the interface as though it was sent from a host directly connected to the interface.

Use the **no** variant of this command to configure PIM to treat only directly connected sources as directly connected.

Syntax

```
ip pim ext-srcs-directly-connected
no ip pim ext-srcs-directly-connected
```

Default The **no** variant of this command is the default behavior.

Mode Interface Configuration for a VLAN interface.

Example To configure PIM to treat all sources as directly connected for VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim ext-srcs-directly-connected
```

To configure PIM to treat only directly connected sources as directly connected for VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip pim ext-srcs-directly-connected
```

ip pim hello-holdtime (PIM-SM)

Overview This command configures a hello-holdtime value. You cannot configure a hello-holdtime value that is less than the current hello-interval.

Use the **no** variant of this command to return it to its default of 3.5 * the current hello-interval.

Syntax

```
ip pim hello-holdtime <holdtime>
no ip pim hello-holdtime
```

Parameter	Description
<holdtime>	<1-65535> The holdtime value in seconds (no fractional seconds are accepted).

Default The default hello-holdtime value is 3.5 * the current hello-interval. The default hello- holdtime is restored using the negated form of this command.

Mode Interface Configuration for a VLAN interface.

Usage Each time the hello interval is updated, the hello holdtime is also updated, according to the following rules:

If the hello holdtime is not configured; or if the hello holdtime is configured and less than the current hello-interval value, it is modified to the (3.5 * hello interval). Otherwise, it retains the configured value.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim hello-holdtime 123
```

ip pim hello-interval (PIM-SM)

Overview This command configures a hello-interval value.

Use the **no** variant of this command to reset the hello-interval to the default.

Syntax

```
ip pim hello-interval <interval>
no ip pim hello-interval
```

Parameter	Description
<interval>	<1-65535> The value in seconds (no fractional seconds accepted).

Default The default hello-interval value is 30 seconds. The default is restored using the negated form of this command.

Mode Interface Configuration for a VLAN interface.

Usage When the hello interval is configured, and the hello holdtime is not configured, or when the configured hello-holdtime value is less than the new hello-interval value; the holdtime value is modified to the (3.5 * hello interval). Otherwise, the hello-holdtime value is the configured value.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim hello-interval 123
```

ip pim ignore-rp-set-priority

Overview Use this command to ignore the RP-SET priority value, and use only the hashing mechanism for RP selection.

This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to disable this setting.

Syntax

```
ip pim ignore-rp-set-priority
no ip pim ignore-rp-set-priority
```

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# ip pim ignore-rp-set-priority
```

ip pim jp-timer

Overview Use this command to set the PIM-SM join/prune timer. Note that the value the device puts into the holdtime field of the join/prune packets it sends to its neighbors is 3.5 times the join/prune timer value set using this command.

Use the **no** variant of this command to return the PIM-SM join/prune timer to its default value of 60 seconds, which corresponds to a join/prune packet holdtime of 210 seconds.

Syntax

```
ip pim jp-timer <1-65535>
no ip pim jp-timer [<1-65535>]
```

Parameter	Description
<1-65535>	Specifies the join/prune timer value. The default value is 60 seconds.

Default The default join/prune timer value is 60 seconds.

Mode Global Configuration

Example To set the join/prune timer value to 300 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip pim jp-timer 300
```

To return the join/prune timer to its default value of 60 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip pim jp-timer
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim neighbor-filter (PIM-SM)

Overview This command enables filtering of neighbors on the VLAN interface. When configuring a neighbor filter, PIM-SM will either not establish adjacency with the neighbor, or terminate adjacency with the existing neighbors if denied by the filtering access list.

Use the **no** variant of this command to disable this function.

Syntax

```
ip pim neighbor-filter {<number>|<accesslist>}
no ip pim neighbor-filter {<number>|<accesslist>}
```

Parameter	Description
<number>	<1-99> Standard IP access-list number.
<accesslist>	IP access list name.

Default By default, there is no filtering.

Mode Interface Configuration for a VLAN interface.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim neighbor-filter 14
```

ip pim register-rate-limit

Overview Use this command to configure the rate of register packets sent by this DR, in units of packets per second.

Use the **no** variant of this command to remove the limit.

Syntax

```
ip pim register-rate-limit <1-65535>
no ip pim register-rate-limit
```

Parameter	Description
<1-65535>	Specifies the maximum number of packets that can be sent per second.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# ip pim register-rate-limit 3444
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim register-rp-reachability

Overview Use this command to enable the RP reachability check for PIM Register processing at the DR. The default setting is no checking for RP-reachability.

Use the **no** variant of this command to disable this processing.

Syntax
```
ip pim register-rp-reachability
no ip pim register-rp-reachability
```

Default This command is disabled; by default, there is no checking for RP-reachability.

Mode Global Configuration

Example
```
awplus# configure terminal
awplus(config)# ip pim register-rp-reachability
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim register-source

Overview Use this command to configure the source address of register packets sent by this DR, overriding the default source address, which is the address of the RPF interface toward the source host.

Use the **no** variant of this command to un-configure the source address of Register packets sent by this DR, reverting back to use the default source address that is the address of the RPF interface toward the source host.

Syntax

```
ip pim register-source [<source-address>|<interface>]
no ip pim register-source
```

Parameter	Description
<source-address>	The IP address, entered in the form A.B.C.D, to be used as the source of the register packets.
<interface>	The name of the interface to be used as the source of the register packets.

Usage notes The configured address must be a reachable address to be used by the RP to send corresponding Register-Stop messages in response. It is normally the local loopback interface address, but can also be a physical address. This address must be advertised by unicast routing protocols on the DR. The configured interface does not have to be PIM enabled.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# ip pim register-source 10.10.1.3
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim register-suppression

Overview Use this command to configure the register-suppression time, in seconds, overriding the default of 60 seconds. Configuring this value modifies register-suppression time at the DR. Configuring this value at the RP modifies the RP-keepalive-period value if the ip pim rp-register-kat command is not used.

Use the **no** variant of this command to reset the value to its default of 60 seconds.

Syntax
```
ip pim register-suppression <1-65535>
no ip pim register-suppression
```

Mode Global Configuration

Example
```
awplus# configure terminal
awplus(config)# ip pim register-suppression 192
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim rp-address

Overview Use this command to statically configure the RP (Rendezvous Point) address for multicast groups.

Use the **no** variant of this command to remove a statically configured RP address for multicast groups.

Syntax

```
ip pim rp-address <ip-address> group-list <group-prefix>
[override]
```

```
no ip pim rp-address <ip-address> group-list <group-prefix>
[override]
```

Parameter	Description
<ip-address>	IP address of RP, entered in the form `A.B.C.D`.
<group-prefix>	Multicast group IP prefix address of RP, entered in the form `A.B.C.D/M`
`override`	Enables statically defined RPs to override dynamically learned RPs.

Mode Global Configuration

Usage notes The AlliedWare Plus PIM-SM implementation supports multiple static RPs. It also supports usage of static RP and the BSR (Bootstrap Router) mechanism simultaneously. The **ip pim rp-address** command is used to statically configure the RP address for multicast groups.

You need to understand the following information before using this command.

If the RP address configured by the BSR, and the statically configured RP address are both available for a group range, then the RP address configured through the BSR is chosen over the statically configured RP address, unless the 'override' parameter is specified, in which case, the static RP will be chosen.

After configuration, the RP address is inserted into a static RP group tree based on the configured group ranges. For each group range, multiple static RPs are maintained in a linked list. This list is sorted in a descending order of IP addresses. When selecting static RPs for a group range, the first element (which is the static RP with highest IP address) is chosen.

RP address deletion is handled by removing the static RP from all the existing group ranges and recalculating the RPs for existing TIB states if required.

NOTE: *A unique RP address may only be specified once as a static RP.*

Example

```
awplus# configure terminal
```

```
awplus(config)# ip pim rp-address 192.0.2.10 group-list
233.252.0.0/24 override
```

Figure 35-2: Output from the **show ip pim sparse-mode rp mapping** command

```
awplus#show ip pim sp rp mapping
PIM Group-to-RP Mappings
Group(s): 233.252.0.0/24, Static
    RP: 192.0.2.10
         Uptime: 00:00:17
```

Related commands

ip pim rp-candidate

ip pim rp-register-kat

show ip pim sparse-mode rp mapping

Command changes

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-0.5: Replaced <acl> parameter with <group-list> parameter.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim rp-candidate

Overview Use this command to make the router an RP (Rendezvous Point) candidate, using the IP address of the specified interface.

Use the **no** variant of this command to remove the RP status set using the **ip pim rp-candidate** command.

Syntax

```
ip pim rp-candidate <interface> [priority <priority> | interval
<interval> | grouplist <grouplist>]
no ip pim rp-candidate [<interface>]
```

Parameter	Description
<interface>	Interface name
<priority>	<0-255> configure priority for an RP candidate.
<interval>	advertisement interval specified in the range <1-16383> (in seconds).
<acl>	The standard, expanded or named ACL to use.

Default The priority value for a candidate RP is 0 by default until specified using the **priority** parameter.

Mode Global Configuration

Usage notes Note that issuing the command **ip pim rp-candidate** *<interface>* without optional **priority**, **interval**, or **grouplist** parameters will configure the candidate RP with a priority value of 0.

Examples To specify a priority of 3, use the following commands:

```
awplus# configure terminal
awplus(config)# ip pim rp-candidate vlan2 priority 3
```

To use the ACL numbered 3 to specify the group prefixes that are advertised in association with the RP address, use the following commands:

```
awplus# configure terminal
awplus(config)# ip pim rp-candidate vlan2 group-list 3
```

To stop the device from being an RP candidate on vlan2 , use the following commands:

```
awplus# configure terminal
awplus(config)# no ip pim rp-candidate vlan2
```

Related commands

ip pim rp-address

ip pim rp-register-kat

ip pim crp-cisco-prefix

Command changes

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim rp-register-kat

Overview Use this command to configure the Keep Alive Time (KAT) for (S,G) states at the RP (Rendezvous Point) to monitor PIM-SM Register packets.

Use the **no** variant of this command to return the PIM-SM KAT timer to its default value of 210 seconds.

Syntax

```
ip pim rp-register-kat <1-65535>
no ip pim rp-register-kat
```

Parameter	Description
<1-65535>	Specify the KAT timer in seconds. The default value is 210 seconds.

Mode Global Configuration

Default The default PIM-SM KAT timer value is 210 seconds.

Examples

```
awplus# configure terminal
awplus(config)# ip pim rp-register-kat 3454
awplus# configure terminal
awplus(config)# no ip pim rp-register-kat
```

Related commands ip pim rp-address

ip pim rp-candidate

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim sparse-mode

Overview Use this command to enable PIM-SM on the VLAN interface.

Use the **no** variant of this command to disable PIM-SM on the VLAN interface.

Syntax

```
ip pim sparse-mode
no ip pim sparse-mode
```

Mode Interface Configuration for a VLAN interface.

Examples

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim sparse-mode
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip pim sparse-mode
```

ip pim sparse-mode join-prune-batching

Overview Use this command to enable batching of Join and Prune messages in PIM-SM. This functionality reduces the number of PIM packets that must be sent to maintain a large number of groups

Use the **no** variant of this command to disable batching of Join and Prune messages in PIM-SM.

Syntax
```
ip pim sparse-mode join-prune-batching
no ip pim sparse-mode join-prune-batching
```

Default Disabled.

Mode Global Configuration

Examples To enable Join/Prune batching for PIM-SM, use the commands:

```
awplus# configure terminal
awplus(config)# ip pim sparse-mode join-prune-batching
```

To disable Join/Prune batching for PIM-SM, use the commands:

```
awplus# configure terminal
awplus(config)# no ip pim sparse-mode join-prune-batching
```

Related commands ip pim sparse-mode wrong-vif-suppression

Command changes Version 5.4.8-2.3: command added.

ip pim sparse-mode passive

Overview Use this command to enable and disable passive mode operation for local members on the VLAN interface.

Use the **no** variant of this command to disable passive mode operation for local members on the VLAN interface.

Syntax

```
ip pim sparse-mode passive
no ip pim sparse-mode passive
```

Mode Interface Configuration for a VLAN interface.

Usage Passive mode essentially stops PIM transactions on the interface, allowing only IGMP mechanism to be active. To turn off passive mode, use the **no ip pim sparse-mode passive** or the ip pim sparse-mode command. To turn off PIM activities on the VLAN interface, use the **no ip pim sparse-mode** command.

Examples

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim sparse-mode passive
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip pim sparse-mode passive
```

ip pim sparse-mode wrong-vif-suppression

Overview Use this command to permit or block multicast packets that arrive on the wrong VLAN Interface (VIF).

Use the **no** variant of this command to disable wrong VIF suppression.

Syntax

```
ip pim sparse-mode wrong-vif-suppression
no ip pim sparse-mode wrong-vif-suppression
```

Default Disabled.

Mode Global Configuration

Usage notes This command enables wrong VIF suppression for PIM sparse-mode. Wrong VIF suppression prevents multicast packets received on the wrong upstream interface from being copied to the CPU.

Examples To enable wrong VIF suppression, use the commands:

```
awplus# configure terminal
awplus(config)# ip pim sparse-mode wrong-vif-suppression
```

To disable wrong VIF suppression, use the commands:

```
awplus# configure terminal
awplus(config)# no ip pim sparse-mode wrong-vif-suppression
```

Related commands ip pim sparse-mode join-prune-batching

Command changes Version 5.4.8-2.3: command added.

ip pim spt-threshold

Overview This command turns on the ability for the last-hop PIM router to switch to SPT (shortest-path tree).

The **no** variant of this command turns off the ability for the last-hop PIM router to switch to SPT.

NOTE: *The switching to SPT happens either at the receiving of the first data packet, or not at all; it is not rate-based.*

Syntax

```
ip pim spt-threshold
no ip pim spt-threshold
```

Mode Global Configuration

Examples To enable the last-hop PIM-SM router to switch to SPT, use the following commands:

```
awplus# configure terminal
awplus(config)# ip pim spt-threshold
```

To stop the last-hop PIM-SM router from being able to switch to SPT, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip pim spt-threshold
```

Related commands ip pim spt-threshold group-list

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim spt-threshold group-list

Overview Use this command to turn on the ability for the last-hop PIM router to switch to SPT (shortest-path tree) for multicast group addresses specified by the given access-list.

The switching to SPT happens either at the receiving of the first data packet, or not at all; it is not rate-based.

Use the **no** variant of this command to turn off switching to the SPT.

Syntax

```
ip pim spt-threshold group-list <acl>
no ip pim spt-threshold group-list [<acl>]
```

Parameter	Description
<acl>	The standard, expanded or named ACL to use.

Mode Global Configuration

Usage notes Turn on/off the ability for the last-hop PIM router to switch to SPT for multicast group addresses specified by the given access-list.

Example

```
awplus# configure terminal
awplus(config)# ip pim spt-threshold group-list 1
awplus(config)# access-list 1 permit 224.0.1.3
```

Related commands ip pim spt-threshold

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

ip pim ssm

Overview Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses. The default keyword defines the SSM range as 232/8.

To define the SSM range to be other than the default, use the access-list parameter option.

Use the **no** variant of this command to disable the SSM range.

Syntax

```
ip pim ssm default
ip pim ssm range {<access-list>|<named-access-list>}
no ip pim ssm
```

Parameter	Description
<access-list>	<1-99> Simple access-list.
<named-access-list>	Named Standard Access List.

Default By default, the command is disabled.

Mode Global Configuration

Usage When an SSM range of IP multicast addresses is defined by the ip pim ssm command, the no (*,G) or (S,G,rpt) state will be initiated for groups in the SSM range.

The messages corresponding to these states will not be accepted or originated in the SSM range.

Examples The following commands show how to configure SSM service for the IP address range defined by access list 10:

```
awplus# configure terminal
awplus(config)# access-list 10 permit 225.1.1.1
awplus(config)# ip pim ssm range 10
```

The following commands show how to set PIM-SSM as default:

```
awplus# configure terminal
awplus(config)# ip pim ssm default
```

The following commands show how to disable PIM-SSM:

```
awplus# configure terminal
awplus(config)# no ip pim ssm
```

service pim

Overview Use this command to enable PIM sparse mode services.

Use the **no** version of the command to disable unused PIM sparse mode services.

Syntax

```
service pim
no service pim
```

Default Enabled

Mode Global Configuration

Usage notes Sometimes it may be desirable to disable unused services, in order to reduce memory use.

Disabling the PIM services will only take effect after you save the configuration and restart the device.

Example To disable the PIM sparse mode service, use the commands:

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

Output Figure 35-3: Example output from **no service pim**

```
awplus(config)#no service pim
% Save the config and restart the device for this change to take
effect
```

Command changes Version 5.5.0-0.1: command added

show debugging pim sparse-mode

Overview This command displays the status of the debugging of the system.

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

Syntax

```
show debugging pim sparse-mode
```

Mode User Exec and Privileged Exec

Example To display PIM-SM debugging settings, use the command:

```
awplus# show debugging pim sparse-mode
```

Figure 35-4: Output from **show debugging pim sparse-mode**

```
Debugging status:
  PIM event debugging is on
  PIM Hello THT timer debugging is on
  PIM event debugging is on
  PIM MFC debugging is on
  PIM state debugging is on
  PIM packet debugging is on
  PIM incoming packet debugging is on
  PIM outgoing packet debugging is on
```

Related commands debug pim sparse-mode

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip pim sparse-mode bsr-router

Overview Use this command to show the Bootstrap Router (BSR) (v2) address.

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

Syntax

```
show ip pim sparse-mode bsr-router
```

Mode User Exec and Privileged Exec

Output Figure 35-5: Output from the **show ip pim sparse-mode bsr-router** command

```
PIMv2 Bootstrap information
  BSR address: 10.10.11.35 (?)
  Uptime:      00:00:38, BSR Priority: 0, Hash mask length: 10
  Expires:     00:01:32
  Role: Non-candidate BSR
  State: Accept Preferred
```

Related commands

show ip pim sparse-mode rp mapping

show ip pim sparse-mode neighbor

Command changes

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip pim sparse-mode interface

Overview Use this command to show PIM-SM interface information.

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

Syntax

```
show ip pim sparse-mode interface
```

Mode User Exec and Privileged Exec

Example To display information about PIM-SM interfaces, use the command:

```
awplus# show ip pim sparse-mode interface
```

Output Figure 35-6: Example output from **show ip pim sparse-mode interface**

```
Total configured interfaces: 16   Maximum allowed: 31
Total active interfaces:     12

Address         Interface VIFindex Ver/   Nbr    DR          DR
                                   Mode   Count  Prior
192.168.1.53    vlan2     0        v2/S   2      2       192.168.1.53
192.168.10.53   vlan3     2        v2/S   0      2       192.168.10.53

... Note that this screen has been edited to remove any additional interfaces.
```

Table 1: Parameters in the output from the **show ip pim sparse-mode interface** command

Parameters	Description
`Total configured interfaces`	The number of configured PIM Sparse Mode interfaces.
`Maximum allowed`	The maximum number of PIM Sparse Mode interfaces that can be configured.
`Total active interfaces`	The number of active PIM Sparse Mode interfaces.
`Address`	Primary PIM-SM address.
`Interface`	Name of the PIM-SM interface.
`VIF Index`	The Virtual Interface index of the VLAN.
`Ver/Mode`	PIM version/Sparse mode.
`Nbr Count`	Neighbor count of the PIM-SM interface.

Table 1: Parameters in the output from the **show ip pim sparse-mode interface** command (cont.)

Parameters	Description
`DR Priority`	Designated Router priority.
`DR`	The IP address of the Designated Router.

Related commands

ip pim sparse-mode

show ip pim sparse-mode rp mapping

show ip pim sparse-mode neighbor

Command changes

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip pim sparse-mode interface detail

Overview Use this command to show detailed information on a PIM-SM interface.

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

Syntax

```
show ip pim sparse-mode interface detail
```

Mode User Exec and Privileged Exec

Output Figure 35-7: Example output from the **show ip pim sparse-mode interface detail** command

```
vlan3 (vif 3):
  Address 192.168.1.149, DR 192.168.1.149
  Hello period 30 seconds, Next Hello in 15 seconds
  Triggered Hello period 5 seconds
  Neighbors:
   192.168.1.22

vlan2 (vif 0):
  Address 10.10.11.149, DR 10.10.11.149
  Hello period 30 seconds, Next Hello in 18 seconds
  Triggered Hello period 5 seconds
  Neighbors:
   10.10.11.4
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip pim sparse-mode local-members

Overview Use this command to show detailed local member information on a VLAN interface configured for PIM-SM. If you do not specify a VLAN interface then detailed local member information is shown for all VLAN interfaces configured for PIM-SM.

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

Syntax

```
show ip pim sparse-mode local-members [<interface>]
```

Parameter	Description
<interface>	Optional. Specify the interface. For instance, VLAN interface `vlan2`.

Mode User Exec and Privileged Exec

Example To show detailed PIM-SM information for all PIM-SM configured VLAN interfaces, use the command:

```
awplus# show ip pim sparse-mode local-members
```

Output Figure 35-8: Example output from the **show ip pim sparse-mode local-members** command

```
awplus#show ip pim sparse-mode local-members
PIM Local membership information

vlan1:
    (*, 224.0.0.4) : Include

vlan203:
    (*, 223.0.0.3) : Include
```

Example To show detailed PIM-SM information for the PIM-SM configured interface vlan1, use the command:

```
awplus# show ip pim sparse-mode local-members vlan1
```

Output Figure 35-9: Example output from the **show ip pim sparse-mode local-members vlan1** command

```
awplus#show ip pim sparse-mode local-members vlan1
PIM Local membership information

vlan1:
    (*, 224.0.0.4) : Include
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip pim sparse-mode mroute

Overview Use this command to display the IP multicast routing table or the IP multicast routing table based on a specific address or addresses.

Syntax

```
show ip pim sparse-mode mroute brief
show ip pim sparse-mode mroute
show ip pim sparse-mode mroute <group-address>
show ip pim sparse-mode mroute <source-address>
show ip pim sparse-mode mroute <source-address> <group-address>
```

Parameter	Description
`brief`	Shows only a summary of the number of each type of multicast entry and the cache.
<group-address>	Group IP address, entered in the form A.B.C.D. Output is all multicast entries belonging to that group.
<source-address>	Source IP address, entered in the form A.B.C.D. Output is all multicast entries belonging to that source.

Mode Privileged Exec

Usage notes Note that when a feature license is enabled, the output for the **show ip pim sparse-mode mroute** command will only show 32 interfaces because of the terminal display width limit. Use the **show ip pim sparse-mode mroute detail** command to display detailed entries of the IP multicast routing table.

Example To display the IP multicast routing table for the address 40.40.40.11, enter the command:

```
awplus# show ip pim sparse-mode mroute 40.40.40.11
```

Output Figure 35-10: Example output from **show ip pim sparse-mode mroute brief**

```
awplus#show ip pim sparse-mode mroute brief
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 99
(S,G,rpt) Entries: 99
FCR Entries: 0
MRIB Msg Cache Hit: 0
```

Output Figure 35-11: Example output from **show ip pim sparse-mode mroute**

```
awplus#show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 99
(S,G,rpt) Entries: 99
FCR Entries: 0
MRIB Msg Cache Hit: 0

(10.200.0.2, 224.1.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
 Local            1
 Joined           0
 Asserted Winner  0
 Asserted Loser   0
 Outgoing         1
  Interop    listener    rx-data     flags (ES,EDW,RXD,DAJ,EOE)
             0x00000000  0x00000000  0x00000001
(10.200.0.2, 224.1.1.1, rpt)
RP: 0.0.0.0
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: RPT NOT JOINED
 Local     0
 Pruned    0
 Outgoing  0
  Interop    listener    rx-data     flags (ES,EDW,RXD,DAJ,EOE)
             0x00000000  0x00000000  0x00000001
...
```

Related commands show ip pim sparse-mode mroute detail

Command changes Version 5.4.7-1.1: VRF-lite support added to SBx8100.

Version 5.4.8-1.1: VRF-lite support added to x930, SBx908 GEN2.

Version 5.4.8-2.1: **brief** parameter added.

show ip pim sparse-mode mroute detail

Overview This command displays detailed entries of the IP multicast routing table, or detailed entries of the IP multicast routing table based on the specified address or addresses.

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

Syntax

```
show ip pim sparse-mode mroute [<group-address>] detail
show ip pim sparse-mode mroute [<source-address>] detail
show ip pim sparse-mode mroute [<group-address>
<source-address>] detail
show ip pim sparse-mode mroute [<source-address>
<group-address>] detail
```

Parameter	Description
<group-address>	Group IP address, entered in the form A.B.C.D. Output is all multicast entries belonging to that group.
<source-address>	Source IP address, entered in the form A.B.C.D. Output is all multicast entries belonging to that source.
detail	Show detailed information.

Usage notes Based on the group and source address, the output is the selected route if present in the multicast route tree.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip pim sparse-mode mroute detail
awplus# show ip pim sparse-mode mroute 40.40.40.11 detail
awplus# show ip pim sparse-mode mroute 224.1.1.1 detail
awplus# show ip pim sparse-mode mroute 224.1.1.1 40.40.40.11
detail
```

Figure 35-12: Example output from the **show ip pim sparse-mode mroute detail** command

```
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 4
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 224.0.1.24) Uptime: 00:06:42
  RP: 0.0.0.0, RPF nbr: None, RPF idx: None
  Upstream:
   State: JOINED, SPT Switch: Disabled, JT: off
   Macro state: Join Desired,
  Downstream:
   vlan2:
     State: NO INFO, ET: off, PPT: off
     Assert State: NO INFO, AT: off
      Winner: 0.0.0.0, Metric: 4294967295l, Pref: 4294967295l,
RPT bit: on
     Macro state: Could Assert, Assert Track
  Local Olist:
   vlan2
```

Command changes

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip pim sparse-mode neighbor

Overview Use this command to show the PIM-SM neighbor information.

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

Syntax

```
show ip pim sparse-mode neighbor [<interface>] [<ip-address>]
[detail]
```

Parameter	Description
<interface>	Interface name (e.g. vlan2). Show neighbors on an interface.
<ip-address>	Show neighbors with a particular address on an interface. The IP address entered in the form A.B.C.D.
detail	Show detailed information.

Mode Privileged Exec

Examples

```
awplus# show ip pim sparse-mode neighbor
awplus# show ip pim sparse-mode neighbor vlan5 detail
```

Figure 35-13: Example output from the **show ip pim sparse-mode neighbor** command

```
Neighbor         Interface   Uptime/Expires    Ver   DR
Address                                              Priority/
Mode
10.10.0.9        vlan2       00:55:33/00:01:44 v2    1 /
10.10.0.136      vlan2       00:55:20/00:01:25 v2    1 /
10.10.0.172      vlan2       00:55:33/00:01:32 v2    1 / DR
192.168.0.100    vlan3       00:55:30/00:01:20 v2    N / DR
```

Figure 35-14: Example output from the **show ip pim sparse-mode neighbor interface detail** command

```
Nbr 10.10.3.180 (vlan5), DR
 Expires in 55 seconds, uptime 00:00:15
 Holdtime: 70 secs, T-bit: off, Lan delay: 1, Override interval:
3
 DR priority: 100, Gen ID: 625159467,
 Secondary addresses:
  192.168.30.1
```

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip pim sparse-mode nexthop

Overview Use this command to see the next hop information as used by PIM-SM.

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

Syntax

```
show ip pim sparse-mode nexthop
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip pim sparse-mode nexthop
```

Figure 35-15: Example output from the **show ip pim sparse-mode nexthop** command

```
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination Type Nexthop Nexthop Nexthop      Nexthop    Metric Pref  Refcnt
                 Num     Addr                 Ifindex    Name
_____________________________________________________________________________
10.10.0.9   .RS.  1      0.0.0.0  4           0           0        1
```

Table 2: Parameters in output of the **show ip pim sparse-mode nexthop** command

Parameter	Description
Destination	The destination address for which PIM-SM requires next hop information.
Type	The type of destination, as indicated by the Flags description. N = New, R= RP, S = Source, U = Unreachable.
Nexthop Num	The number of next hops to the destination. PIM-SM always uses only 1 next hop.
Nexthop Addr	The address of the primary next hop gateway.
Nexthop IfIndex	The interface on which the next hop gateway can be reached.
Nexthop Name	The name of next hop interface.
Metric	The metric of the route towards the destination.
Preference	The preference of the route towards destination.
Refcnt	Only used for debugging.

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip pim sparse-mode packet statistics

Overview Use this command to display the current packet receive counts for PIM sparse-mode.

Syntax

```
show ip pim sparse-mode packet statistics
```

Mode Privileged Exec

Example The following command displays the current packet receive counts for PIM sparse-mode:

```
awplus# configure terminal
awplus(config)# show ip pim sparse-mode statistics
```

Output Figure 35-16: Example output from **show ip pim sparse-mode statistics**

```
awplus(config)#show ip pim sparse-mode statistics
PIM-SM Receive Packet Statistics :
All PIM-SM    :   Total : 25   Valid : 25
Hello         :   Total : 14   Valid : 14
Register      :   Total : 5   Valid : 5
Register Stop :   Total : 0   Valid : 0
Join/Prune    :   Total : 0   Valid : 0
Bootstrap     :   Total : 6   Valid : 6
Assert        :   Total : 0   Valid : 0
Candidate-RP  :   Total : 0   Valid : 0
```

Related commands clear ip pim sparse-mode packet statistics

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip pim sparse-mode rp-hash

Overview Use this command to display the Rendezvous Point (RP) to be chosen based on the group selected.

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

Syntax

```
show ip pim sparse-mode rp-hash <group-addr>
```

Parameter	Description
<group-addr>	The group address for which to find the RP, entered in the form A.B.C.D.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip pim sparse-mode rp-hash 224.0.1.3
```

Figure 35-17: Output from the **show ip pim sparse-mode rp-hash** command

```
RP: 10.10.11.35
Info source: 10.10.11.35, via bootstrap
```

Related commands show ip pim sparse-mode rp mapping

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

show ip pim sparse-mode rp mapping

Overview Use this command to show group-to-RP (Rendezvous Point) mappings, and the RP set.

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

Syntax

```
show ip pim sparse-mode rp mapping
```

Mode Privileged Exec

Example

```
awplus# show ip pim sparse-mode rp mapping
```

Figure 35-18: Output from the **show ip pim sparse-mode rp mapping** command

```
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
  RP: 10.10.0.9
    Info source: 10.10.0.9, via bootstrap, priority 192
         Uptime: 16:52:39, expires: 00:02:50
```

Related commands show ip pim sparse-mode rp-hash

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

undebug all pim sparse-mode

Overview Use this command to disable all PIM-SM debugging.

Syntax
```
undebug all pim sparse-mode
```

Mode Privileged Exec

Example
```
awplus# undebug all pim sparse-mode
```

Related commands debug pim sparse-mode

Command changes Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

36 PIM-SMv6 Commands

Introduction

Overview

This chapter provides an alphabetical reference of PIM-SMv6 commands. For IPv6 Multicast commands, see Multicast Commands. For an overview of PIM-SMv6, see the PIM-SMv6 Feature Overview and Configuration Guide.

IPv6 must be enabled on an interface with the ipv6 enable command, IPv6 forwarding must be enabled globally for routing IPv6 with the ipv6 forwarding command, and IPv6 multicasting must be enabled globally with the ipv6 multicast-routing command before using PIM-SMv6 commands.

Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the clear ipv6 mroute command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous IPv6 static multicast routes.

NOTE: *The IPv6 Multicast addresses shown can be derived from IPv6 unicast prefixes as per RFC 3306.The IPv6 unicast prefix reserved for documentation is 2001:0db8::/32 as per RFC 3849. Using the base /32 prefix the IPv6 multicast prefix for 2001:0db8::/32 is ff3x:20:2001:0db8::/64. Where an RP address is 2001:0db8::1 the embedded RP multicast prefix is ff7x:120:2001:0db8::/96. For ASM (Any-Source Multicast) the IPV6 multicast addresses allocated for documentation purposes are ff0x::0db8:0:0/96 as per RFC 6676. This is a /96 prefix so that it can be used with group IDs as per RFC 3307. These addresses should not be used for practical networks (other than for testing purposes), nor should they appear in any public network.*

The IPv6 addresses shown use the address space 2001:0db8::/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical networks (other than for testing purposes) nor should they appear on any public network.

Command List

- "clear ipv6 mroute pim" on page 1813
- "clear ipv6 mroute pim sparse-mode" on page 1814
- "clear ipv6 pim sparse-mode bsr rp-set *" on page 1815
- "debug ipv6 pim sparse-mode" on page 1816

- "debug ipv6 pim sparse-mode packet" on page 1818
- "debug ipv6 pim sparse-mode timer" on page 1819
- "ipv6 pim accept-register" on page 1821
- "ipv6 pim anycast-rp" on page 1822
- "ipv6 pim bsr-border" on page 1823
- "ipv6 pim bsr-candidate" on page 1824
- "ipv6 pim cisco-register-checksum" on page 1825
- "ipv6 pim cisco-register-checksum group-list" on page 1826
- "ipv6 pim crp-cisco-prefix" on page 1827
- "ipv6 pim dr-priority" on page 1828
- "ipv6 pim exclude-genid" on page 1829
- "ipv6 pim ext-srcs-directly-connected" on page 1830
- "ipv6 pim hello-holdtime" on page 1831
- "ipv6 pim hello-interval" on page 1832
- "ipv6 pim ignore-rp-set-priority" on page 1833
- "ipv6 pim jp-timer" on page 1834
- "ipv6 pim neighbor-filter" on page 1835
- "ipv6 pim register-rate-limit" on page 1836
- "ipv6 pim register-rp-reachability" on page 1837
- "ipv6 pim register-source" on page 1838
- "ipv6 pim register-suppression" on page 1839
- "ipv6 pim rp-address" on page 1840
- "ipv6 pim rp-candidate" on page 1842
- "ipv6 pim rp embedded" on page 1844
- "ipv6 pim rp-register-kat" on page 1845
- "ipv6 pim sparse-mode" on page 1846
- "ipv6 pim sparse-mode passive" on page 1847
- "ipv6 pim spt-threshold" on page 1848
- "ipv6 pim spt-threshold group-list" on page 1849
- "ipv6 pim ssm" on page 1850
- "ipv6 pim unicast-bsm" on page 1851
- "service pim6" on page 1852
- "show debugging ipv6 pim sparse-mode" on page 1853
- "show ipv6 pim sparse-mode bsr-router" on page 1854
- "show ipv6 pim sparse-mode interface" on page 1855

- "show ipv6 pim sparse-mode interface detail" on page 1857
- "show ipv6 pim sparse-mode local-members" on page 1858
- "show ipv6 pim sparse-mode mroute" on page 1860
- "show ipv6 pim sparse-mode mroute detail" on page 1862
- "show ipv6 pim sparse-mode neighbor" on page 1864
- "show ipv6 pim sparse-mode nexthop" on page 1865
- "show ipv6 pim sparse-mode rp-hash" on page 1866
- "show ipv6 pim sparse-mode rp mapping" on page 1867
- "show ipv6 pim sparse-mode rp nexthop" on page 1868
- "undebug all ipv6 pim sparse-mode" on page 1870
- "undebug ipv6 pim sparse-mode" on page 1871

clear ipv6 mroute pim

Overview Use this command to clear all Multicast Forwarding Cache (MFC) entries in PIM-SMv6.

NOTE: *Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the clear ipv6 mroute command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous static IPv6 multicast routes.*

Syntax

```
clear ipv6 mroute [*] pim sparse-mode
```

Parameter	Description
*	Clears all PIM-SMv6 multicast routes. Using this command without this optional operator only deletes the multicast router table entries.

Mode Privileged Exec

Example

```
awplus# clear ipv6 mroute pim sparse-mode
awplus# clear ipv6 mroute * pim sparse-mode
```

clear ipv6 mroute pim sparse-mode

Overview Use this command to clear all multicast route table entries learned through PIM-SMv6 for a specified multicast group address, and optionally a specified multicast source address.

NOTE: *Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the clear ipv6 mroute command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous static IPv6 multicast routes.*

Syntax

```
clear ipv6 mroute <Group-IPv6-add> pim sparse-mode
clear ipv6 mroute <Group-IPv6-add> <Source-IPv6-add> pim
sparse-mode
```

Parameter	Description
<Group-IPv6-add>	Specify a multicast group IPv6 address, entered in the form X:X::X:X.
<Source-IPv6-add>	Specify a source group IPv6 address, entered in the form X:X::X:X.

Mode Privileged Exec

Example

```
awplus# clear ipv6 mroute 2001:db8:: pim sparse-mode
awplus# clear ipv6 mroute 2001:db8:: 2002:db8:: pim sparse-mode
```

clear ipv6 pim sparse-mode bsr rp-set *

Overview Use this command to clear all Rendezvous Point (RP) sets learned through the PIM-SMv6 Bootstrap Router (BSR).

NOTE: *Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the clear ipv6 mroute command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous static IPv6 multicast routes.*

Syntax

```
clear ipv6 pim sparse-mode bsr rp-set *
```

Parameter	Description
*	Clears all RP sets.

Mode Privileged Exec

Usage For multicast clients, note that one router will be automatically or statically designated as the RP, and all routers must explicitly join through the RP. A Designated Router (DR) sends periodic Join/Prune messages toward a group-specific RP for each group that it has active members.

For multicast sources, note that the Designated Router (DR) unicasts Register messages to the RP encapsulating the data packets from the multicast source. The RP forwards decapsulated data packets toward group members.

Example

```
awplus# clear ipv6 pim sparse-mode bsr rp-set *
```

debug ipv6 pim sparse-mode

Overview Use this command to activate PIM-SMv6 debugging.

Use the no variant of this command to deactivate PIMv6 debugging. Note that the undebug ipv6 pim sparse-mode command is an alias of the no variant of this command.

Syntax

```
debug ipv6 pim sparse-mode [all] [events] [mfc] [mib] [nexthop]
[nsm] [state] [timer]
```

```
no debug ipv6 pim sparse-mode [all] [events] [mfc] [mib]
[nexthop] [nsm] [state] [timer]
```

Parameter	Description
`all`	Activates/deactivates all PIM-SMv6 debugging.
`events`	Activates debug printing of PIM-SMv6 events.
`mfc`	Activates debug printing of MFC (Multicast Forwarding Cache).
`mib`	Activates debug printing of PIM-SMv6 MIBs.
`nexthop`	Activates debug printing of PIM-SMv6 next hop communications.
`nsm`	Activates debugging of PIM-SMv6 NSM (Network Services Module) communications.
`state`	Activates debug printing of state transition on all PIM-SMv6 FSMs.
`timer`	Activates debug printing of PIM-SMv6 timers.

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# debug ipv6 pim sparse-mode all
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# debug ipv6 pim sparse-mode events
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# debug ipv6 pim sparse-mode nexthop
```

Validation output

Figure 36-1: Example output from the **show debugging ipv6 pim sparse-mode** command after issuing **multiple debug ipv6 pim sparse-mode** commands

```
awplus#debug ipv6 pim sparse-mode state
awplus#debug ipv6 pim sparse-mode events
awplus#debug ipv6 pim sparse-mode packet
awplus#show debugging ipv6 pim sparse-mode
PIM-SMv6 debugging status:
  PIM event debugging is on
  PIM MFC debugging is off
  PIM state debugging is on
  PIM packet debugging is on
  PIM Hello HT timer debugging is off
  PIM Hello NLT timer debugging is off
  PIM Hello THT timer debugging is off
  PIM Join/Prune JT timer debugging is off
  PIM Join/Prune ET timer debugging is off
  PIM Join/Prune PPT timer debugging is off
  PIM Join/Prune KAT timer debugging is off
  PIM Join/Prune OT timer debugging is off
  PIM Assert AT timer debugging is off
  PIM Register RST timer debugging is off
  PIM Bootstrap BST timer debugging is off
  PIM Bootstrap CRP timer debugging is off
  PIM mib debugging is off
  PIM nsm debugging is off
  PIM nexthop debugging is off
```

Related commands

show debugging ipv6 pim sparse-mode

undebug all ipv6 pim sparse-mode

undebug ipv6 pim sparse-mode

debug ipv6 pim sparse-mode packet

Overview Use this command to activate PIM-SMv6 packet debugging.

Use the no variant of this command to deactivate PIMv6 packet debugging.

Syntax

```
debug ipv6 pim sparse-mode packet {in|out}
no debug ipv6 pim sparse-mode packet {in|out}
```

Parameter	Description
`packet`	Activates debug printing of incoming and/or outgoing IPv6 packets.
`in`	Specify incoming packet debugging.
`out`	Specify outgoing packet debugging.

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# debug ipv6 pim sparse-mode packet in
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# debug ipv6 pim sparse-mode packet out
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# no debug ipv6 pim sparse-mode packet in
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# no debug ipv6 pim sparse-mode packet out
```

Related commands

show debugging ipv6 pim sparse-mode

undebug all ipv6 pim sparse-mode

debug ipv6 pim sparse-mode timer

Overview Use this command to enable debugging for the specified PIM-SMv6 timers.

Use the **no** variants of this command to disable debugging for the specified PIM-SMv6 timers.

Syntax

```
debug ipv6 pim sparse-mode timer assert [at]
no debug ipv6 pim sparse-mode timer assert [at]
debug pim ipv6 sparse-mode timer bsr [bst|crp]
no debug pim ipv6 sparse-mode timer bsr [bst|crp]
debug pim ipv6 sparse-mode timer hello [ht|nlt|tht]
no debug pim ipv6 sparse-mode timer hello [ht|nlt|tht]
debug pim ipv6 sparse-mode timer joinprune [jt|et|ppt|kat|ot]
no debug pim ipv6 sparse-mode timer joinprune
[jt|et|ppt|kat|ot]
debug pim ipv6 sparse-mode timer register [rst]
no debug pim ipv6 sparse-mode timer register [rst]
```

Parameter	Description
`assert`	Enable or disable debugging for the Assert timers.
`at`	Enable or disable debugging for the Assert Timer.
`bsr`	Enable or disable debugging for the specified Bootstrap Router timer, or all Bootstrap Router timers.
`bst`	Enable or disable debugging for the Bootstrap Router: Bootstrap Timer.
`crp`	Enable or disable debugging for the Bootstrap Router: Candidate-RP Timer.
`hello`	Enable or disable debugging for the specified Hello timer, or all Hello timers.
`ht`	Enable or disable debugging for the Hello timer: Hello Timer.
`nlt`	Enable or disable debugging for the Hello timer: Neighbor Liveness Timer.
`tht`	Enable or disable debugging for the Hello timer: Triggered Hello Timer.
`joinprune`	Enable or disable debugging for the specified JoinPrune timer, or all JoinPrune timers.
`jt`	Enable or disable debugging for the JoinPrune timer: upstream Join Timer.
`et`	Enable or disable debugging for the JoinPrune timer: Expiry Timer.
`ppt`	Enable or disable debugging for the JoinPrune timer: PrunePending Timer.

Parameter	Description
`kat`	Enable or disable debugging for the JoinPrune timer: KeepAlive Timer.
`ot`	Enable or disable debugging for the JoinPrune timer: Upstream Override Timer.
`register`	Enable or disable debugging for the Register timers.
`rst`	Enable or disable debugging for the Register timer: Register Stop Timer.

Default By default, all debugging is disabled.

Mode Privileged Exec and Global Configuration

Examples To enable debugging for the PIM-SMv6 Bootstrap Router bootstrap timer, use the commands:

```
awplus(config)# debug ipv6 pim sparse-mode timer bsr bst
```

To enable debugging for the PIM-SMv6 Hello: neighbor liveness timer, use the command:

```
awplus(config)# debug ipv6 pim sparse-mode timer hello ht
```

To enable debugging for the PIM-SMv6 Joinprune expiry timer, use the command:

```
awplus# debug ipv6 pim sparse-mode timer joinprune et
```

To disable debugging for the PIM-SMv6 Register timer, use the command:

```
awplus# no debug ipv6 pim sparse-mode timer register
```

Related commands show debugging ipv6 pim sparse-mode

ipv6 pim accept-register

Overview Use this command to configure the ability to filter out multicast sources specified by the given software IPv6 access-list at the Rendezvous Point (RP), so that the RP will accept/refuse to perform the register mechanism for the packets sent by the specified sources. By default, the RP accepts register packets from all multicast sources.

Use the **no** variant of this command to revert to default.

Syntax

```
ipv6 pim accept-register list{<access-list>}
no ipv6 pim accept-register
```

Parameter	Description
<access-list>	Specify a Standard or an Extended software IPv6 Access list. See IPv6 Software Access Control List (ACL) Commands for supported IPv6 ACLs.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim accept-register list G2
awplus(config)# ipv6 access-list standard G2 permit
2001:db8::/128
awplus# configure terminal
awplus(config)# no ipv6 pim accept-register
```

ipv6 pim anycast-rp

Overview Use this command to configure Anycast RP (Rendezvous Point) in an RP set.

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

Syntax

```
ipv6 pim anycast-rp <anycast-rp-address> <member-rp-address>
no ipv6 pim anycast-rp <anycast-rp-address>
[<member-rp-address>]
```

Parameter	Description
<anycast-rp-address>	<X:X::X:X> Specify an Anycast IPv6 address to configure an Anycast RP (Rendezvous Point) in a RP set.
<member-rp-address>	<A:B::C:D> Specify an Anycast RP (Rendezvous Point)IPv6 address to configure an Anycast RP in a RP set.

Mode Global Configuration

Usage notes Anycast is a network addressing and routing scheme where data is routed to the nearest or best destination as viewed by the routing topology. Compared to unicast with a one-to-one association between network address and network endpoint, and multicast with a one-to-many association between network address and network endpoint; anycast has a one-to-many association between network address and network endpoint. For anycast, each destination address identifies a set of receiver endpoints, from which only one receiver endpoint is chosen.

Use this command to specify the Anycast RP configuration in the Anycast RP set. Use the **no** variant of this command to remove the Anycast RP configuration. Note that the member RP address is optional when using the **no** parameter to remove the Anycast RP configuration. removing the anycast RP address also removes the member RP address.

Examples The following example shows how to configure the Anycast RP address with **ipv6 pim anycast-rp**:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim anycast-rp 2:2::2:2 20:20::20:20
```

The following example shows how to remove the Anycast RP in the RP set specifying only the anycast RP address with **no ipv6 pim anycast-rp**, but not specifying the member RP address:

```
awplus# configure terminal
awplus(config)# no ipv6 pim anycast-rp 2:2::2:2 20:20::20:20
```

ipv6 pim bsr-border

Overview Use the **ipv6 pim bsr-border** command to prevent Bootstrap Router (BSR) messages from being sent or received through a VLAN interface. The BSR border is the border of the PIM-SMv6 domain.

Use the **no** variant of this command to disable the configuration set with **ipv6 pim bsr-border**.

Syntax

```
ipv6 pim bsr-border
no ipv6 pim bsr-border
```

Mode Interface Configuration for a VLAN interface.

Usage When this command is configured on a VLAN interface, no PIM-SMv6 BSR messages will be sent or received through the interface. Configure an interface bordering another PIM- SMv6 domain with this command to avoid BSR messages from being exchanged between the two PIM-SMv6 domains.

BSR messages should not be exchanged between different domains, because devices in one domain may elect Rendezvous Points (RPs) in the other domain, resulting in loss of isolation between the two PIM domains that would stop the PIM-SMv6 protocol from working as intended.

Examples The following example configures the VLAN interface vlan2 to be the PIM-SMv6 domain border:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim bsr-border
```

The following example removes the VLAN interface vlan2 from the PIM-SMv6 domain border:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 pim bsr-border
```

ipv6 pim bsr-candidate

Overview Use this command to give the device the candidate BSR (Bootstrap Router) status using the specified IPv6 address mask of the interface.

Use the **no** variant of this command to withdraw the address of the interface from being offered as a BSR candidate.

Syntax

```
ipv6 pim bsr-candidate <interface> [<hash>] [<priority>]
no ipv6 pim bsr-candidate [<interface>]
```

Parameter	Description
<interface>	Specify the interface. For instance, VLAN interface `vlan2`.
<hash>	<0-128> configure the hash mask length used for RP selection. The default hash value if you do not configure this parameter is 126.
<priority>	<0-255> configure priority for a BSR candidate. Note that you must also specify the *<hash>* (mask length) when specifying the *<priority>*. The default priority if you do not configure this parameter is 64.

Mode Global Configuration

Default The default hash parameter value is 126 and the default priority parameter value is 64.

Examples To set the BSR candidate to the VLAN interface vlan2, with the optional mask length and BSR priority parameters, enter the commands shown below:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim bsr-candidate vlan2 20 30
```

To withdraw the address of vlan2 from being offered as a BSR candidate, enter:

```
awplus# configure terminal
awplus(config)# no ipv6 pim bsr-candidate vlan2
```

ipv6 pim cisco-register-checksum

Overview Use this command to configure the option to calculate the Register Checksum over the whole packet. This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to disable this option.

Syntax
```
ipv6 pim cisco-register-checksum
no ipv6 pim cisco-register-checksum
```

Default This command is disabled by default. By default, Register Checksum is calculated only over the header.

Mode Global Configuration

Example
```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim cisco-register-checksum
awplus# configure terminal
awplus(config)# no ipv6 pim cisco-register-checksum
```

ipv6 pim cisco-register-checksum group-list

Overview Use this command to configure the option to calculate the Register Checksum over the whole packet on multicast groups as specified by the software IPv6 access-list. This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to revert to default settings.

Syntax

```
ipv6 pim cisco-register-checksum group-list <IPv6-access-list>
no ipv6 pim cisco-register-checksum group-list
<IPv6-access-list>
```

Parameter	Description
<IPv6-access-list>	Optional. Specify a Standard or Extended software IPv6 access list. See IPv6 Software Access Control List (ACL) Commands for supported IPv6 ACLs. Use this parameter to configure the option to calculate the Register Checksum over the whole packet on multicast groups as specified by an IPv6 access list entered after this command.

Mode Global Configuration

Default This command is disabled by default. By default, Register Checksum is calculated only over the header.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim cisco-register-checksum group-list G1
awplus(config)# ipv6 access-list standard G1 permit
ff0x::db8:0:0/96
```

ipv6 pim crp-cisco-prefix

Overview Use this command to interoperate with Cisco devices that conform to an earlier draft standard. Some Cisco devices might not accept candidate RPs with a group prefix number of zero. Note that the latest BSR specification prohibits sending RP advertisements with prefix 0.

Use the **no** variant of this command to revert to the default settings.

Syntax
```
ipv6 pim crp-cisco-prefix
no ipv6 pim crp-cisco-prefix
```

Mode Global Configuration

Usage Cisco's BSR code does not conform to the latest BSR draft, it does not accept candidate RPs with a group prefix number of zero. To make the candidate RP work with a Cisco BSR, use the **ipv6 pim crp-cisco-prefix** command when interoperating with older versions of Cisco IOS.

Example
```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim crp-cisco-prefix
awplus# configure terminal
awplus(config)# no ipv6 pim crp-cisco-prefix
```

Related commands ipv6 pim rp-candidate

ipv6 pim dr-priority

Overview Use this command to set the Designated Router priority value.

Use the **no** variant of this command to disable this function.

Syntax

```
ipv6 pim dr-priority  <priority>
no ipv6 pim dr-priority [<priority>]
```

Parameter	Description
<priority>	<0-4294967294> Specify the Designated Router priority value. Note that a higher value has a higher preference or higher priority.

Default The default value is 1. The negated form of this command restores the value to the default.

Mode Interface Configuration for a VLAN interface.

Examples To set the Designated Router priority value to 11234 for the VLAN interface vlan2, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim dr-priority 11234
```

To disable the Designated Router priority value for the VLAN interface vlan2, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 pim dr-priority
```

Related commands ipv6 pim ignore-rp-set-priority

ipv6 pim exclude-genid

Overview Use this command to exclude the GenID option from Hello packets sent out by the PIM-SMv6 module on a particular interface. This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to revert to default settings.

Syntax
```
ipv6 pim exclude-genid
no ipv6 pim exclude-genid
```

Default By default, this command is disabled; the GenID option is included.

Mode Interface Configuration for a VLAN interface.

Examples
```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim exclude-genid
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 pim exclude-genid
```

ipv6 pim ext-srcs-directly-connected

Overview Use this command to configure PIM-SMv6 to treat all source traffic arriving on the interface as though it was sent from a host directly connected to the interface.

Use the **no** variant of this command to configure PIM-SMv6 to treat only directly connected sources as directly connected.

Syntax

```
ipv6 pim ext-srcs-directly-connected
no ipv6 pim ext-srcs-directly-connected
```

Default The **no** variant of this command is the default behavior.

Mode Interface Configuration for a VLAN interface.

Example To configure PIM-SMv6 to treat all sources as directly connected for VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim ext-srcs-directly-connected
```

To configure PIM-SMv6 to treat only directly connected sources as directly connected for VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 pim ext-srcs-directly-connected
```

ipv6 pim hello-holdtime

Overview This command configures a hello-holdtime value. You cannot configure a hello-holdtime value that is less than the current hello-interval.

Use the **no** variant of this command to return it to its default of 3.5 * the current hello-interval.

Syntax

```
ipv6 pim hello-holdtime <holdtime>
no ipv6 pim hello-holdtime
```

Parameter	Description
<holdtime>	<1-65535> The holdtime value in seconds (no fractional seconds are accepted).

Default The default hello-holdtime value is 3.5 * the current hello-interval. The default hello- holdtime is restored using the negated form of this command.

Mode Interface Configuration for a VLAN interface.

Usage Each time the hello interval is updated, the hello holdtime is also updated, according to the following rules:

If the hello holdtime is not configured; or if the hello holdtime is configured and less than the current hello-interval value, it is modified to the (3.5 * hello interval). Otherwise, it retains the configured value.

Examples

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim hello-holdtime 123
```

ipv6 pim hello-interval

Overview This command configures a hello-interval value for PIM-SMv6.

Use the **no** variant of this command to reset the hello-interval for PIM-SMv6 to the default.

Syntax

```
ipv6 pim hello-interval <interval>
no ipv6 pim hello-interval
```

Parameter	Description
<interval>	<1-65535> The value in seconds (no fractional seconds accepted).

Default The default hello-interval value is 30 seconds. The default is restored using the negated form of this command.

Mode Interface Configuration for a VLAN interface.

Usage When the hello interval is configured, and the hello holdtime is not configured, or when the configured hello-holdtime value is less than the new hello-interval value; the holdtime value is modified to the (3.5 * hello interval). Otherwise, the hello-holdtime value is the configured value.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim hello-interval 123
```

ipv6 pim ignore-rp-set-priority

Overview Use this command to ignore the RP-SET priority value, and use only the hashing mechanism for RP selection.

Use the **no** variant of this command to disable this setting.

Syntax

```
ipv6 pim ignore-rp-set-priority
no ipv6 pim ignore-rp-set-priority
```

Mode Global Configuration

Usage This command is used to inter-operate with older Cisco IOS versions.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim ignore-rp-set-priority
awplus# configure terminal
awplus(config)# no ipv6 pim ignore-rp-set-priority
```

ipv6 pim jp-timer

Overview Use this command to set the PIM-SMv6 join/prune timer. Note that the value set by the join/prune timer is the value that the device puts into the holdtime field of the join/prune packets it sends to its neighbors.

Use the **no** variant of this command to return the PIM-SMv6 join/prune timer to its default value of 210 seconds.

Syntax

```
ipv6 pim jp-timer <1-65535>
no ipv6 pim jp-timer [<1-65535>]
```

Parameter	Description
<1-65535>	Specifies the Join/Prune timer value. The default value is 210 seconds.

Default The default PIM-SMv6 join/prune timer value is 210 seconds.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim jp-timer 300
awplus# configure terminal
awplus(config)# no ipv6 pim jp-timer
```

ipv6 pim neighbor-filter

Overview This command enables filtering of neighbors on the VLAN interface. When configuring a neighbor filter, PIM-SMv6 will either not establish adjacency with the neighbor, or terminate adjacency with the existing neighbors if denied by the filtering IPv6 access list.

Use the **no** variant of this command to disable this function.

Syntax

```
ipv6 pim neighbor-filter <IPv6-accesslist>
no ipv6 pim neighbor-filter <IPv6-accesslist>
```

Parameter	Description
<IPv6-accesslist>	Specify a Standard or an Extended software IPv6 access list name for the PIM-SMv6 neighbor filter. See the IPv6 Software Access Control List (ACL) Commands chapter for supported IPv6 ACLs.

Default By default, there is no neighbor filtering applied to an interface.

Mode Interface Configuration for a VLAN interface.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config)# ipv6 enable
awplus(config-if)# ipv6 pim neighbor-filter filter1
awplus(config-if)# ipv6 access-list standard filter1 deny
fe80:20e:cff:fe01:facc
awplus(config-if)# ipv6 access-list standard filter1 permit any
awplus(config-if)# exit
```

ipv6 pim register-rate-limit

Overview Use this command to configure the rate of register packets sent by this DR, in units of packets per second. The configured rate is per (S, G) state, and is not a system wide rate.

Use the **no** variant of this command to remove the limit and reset to the default rate limit.

Syntax

```
ipv6 pim register-rate-limit <1-65535>
no ipv6 pim register-rate-limit
```

Parameter	Description
<1-65535>	Specifies the maximum number of packets that can be sent per second.

Mode Global Configuration

Default The default is 0, as reset with the **no** variant, which also specifies an unlimited rate limit.

Examples

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim register-rate-limit 3444
awplus# configure terminal
awplus(config)# no ipv6 pim register-rate-limit 3444
```

ipv6 pim register-rp-reachability

Overview Use this command to enable the RP reachability check for PIMv6 Register processing at the DR. The default setting is no checking for RP-reachability.

Use the **no** variant of this command to disable this processing.

Syntax
```
ipv6 pim register-rp-reachability
no ipv6 pim register-rp-reachability
```

Default This command is disabled; by default, there is no checking for RP-reachability.

Mode Global Configuration

Examples
```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim register-rp-reachability
awplus# configure terminal
awplus(config)# no ipv6 pim register-rp-reachability
```

ipv6 pim register-source

Overview Use this command to configure the source IPv6 address of register packets sent by this DR, overriding the default source IPv6 address, which is the IPv6 address of the RPF interface toward the source host.

Use the **no** variant of this command to remove the IPv6 source address of Register packets sent by this DR, reverting back to use the default IPv6 source address that is the address of the RPF interface toward the source host.

Syntax

```
ipv6 pim register-source [<source-IPv6-address>|<interface>]
no ipv6 pim register-source
```

Parameter	Description
<source-IPv6-address>	The IPv6 address, entered in the form X:X::X:X, to be used as the source of the register packets.
<interface>	The name of the VLAN interface to be used as the source of the register packets.

Usage The configured address must be a reachable address to be used by the RP to send corresponding Register-Stop messages in response. It is normally the local loopback IPv6 interface address, but can also be a physical IPv6 address. This IPv6 address must be advertised by unicast routing protocols on the DR. The configured interface does not have to be PIM-SMv6 enabled.

Mode Global Configuration

Examples

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim register-source 3ffe::24:2
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim register-source vlan2
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# no ipv6 pim register-source
```

ipv6 pim register-suppression

Overview Use this command to configure the register-suppression time, in seconds, overriding the default of 60 seconds.

Use the **no** variant of this command to reset the value to its default of 60 seconds.

Syntax

```
ipv6 pim register-suppression <1-65535>
no ipv6 pim register-suppression
```

Parameter	Description
<1-65535>	Register suppression on time in seconds.

Mode Global Configuration

Default The default PIM-SMv6 register suppression time is 60 seconds, and is restored with the no variant of this command.

Usage Configuring this value modifies register-suppression time at the DR. Configuring this value at the RP modifies the RP-keepalive-period value if the ipv6 pim rp-register-kat command is not used.

Examples

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim register-suppression 192
awplus# configure terminal
awplus(config)# no ipv6 pim register-suppression
```

ipv6 pim rp-address

Overview Use this command to statically configure RP (Rendezvous Point) address for IPv6 multicast groups.

Use the **no** variant of this command to remove a statically configured RP (Rendezvous Point) address for IPv6 multicast groups.

Syntax

```
ipv6 pimv6 rp-address <IPv6-address> [<IPv6-access-list>]
[override]
```

```
no ipv6 pim rp-address <IPv6-address> [<IPv6-access-list>]
[override]
```

Parameter	Description
<IPv6-address>	Specify the IPv6 address of the Rendezvous Point, entered in the form `X:X::X:X`.
<IPv6-access-list>	Specify a Standard or an Extended software IPv6 access-list name. See IPv6 Software Access Control List (ACL) Commands for supported IPv6 ACLs.
`override`	Specify this optional parameter keyword to enable any statically defined RPs to override dynamically learned RPs.

Mode Global Configuration

Usage notes The AlliedWare Plus™ PIM-SMv6 implementation supports multiple static RPs. It also supports usage of static-RP and BSR mechanism simultaneously. The **ipv6 pim rp-address** command is used to statically configure the RP address for IPv6 multicast groups.

You need to understand the following information before using this command.

If the RP-address that is configured by the BSR, and the RP-address that is configured statically, are both available for a group range, then the RP-address configured through BSR is chosen over the statically configured RP-address.

A single static-RP can be configured for multiple group ranges using software IPv6 access- lists (ACLs). However, configuring multiple static RPs (using **ipv6 pim rp-address** command) with the same RP address is not allowed. The static-RP can either be configured for the whole multicast group range `ff00::/8` (without using IPv6 ACLs) or for specific group ranges (when using IPv6 ACLs).

For example, configuring **ipv6 pim rp-address 3ffe:10:10:5::153** will configure static-RP `3ffe:10:10:5::153` for the default group range `ff00::/8`. Configuring **ipv6 pim rp-address 3ffee:20:20:5::153 grp-list** will configure static-RP `3ffe:20:20:5::153` for all the group ranges represented by permit filters in the defined named **grp-list** ACL.

If multiple static-RPs are available for a group range, then one with the highest IPv6 address is chosen.

Only `permit` filters in IPv6 ACL are considered as valid group ranges. The default `permit` filter `::/0` is converted to the default multicast filter `ff00::/8`.

After configuration, the RP-address is inserted into a static-RP group tree based on the configured group ranges. For each group range, multiple static-RPs are maintained in a list. This list is sorted in a descending order of IPv6 addresses. When selecting static-RPs for a group range, the first element (which is the static-RP with highest IPv6 address) is chosen.

RP-address deletion is handled by removing the static-RP from all the existing group ranges and recalculating the RPs for existing TIB states if required.

Group mode and RP address mappings learned through BSR take precedence over mappings statistically defined by the ipv6 pim rp-address command. Commands with the override keyword take precedence over dynamically learned mappings.

Examples

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard G2 permit
2001:db8::/128
awplus(config)# ipv6 pim rp-address 3ffe:30:30:5::153 G2
awplus# configure terminal
awplus(config)# no ipv6 pim rp-address 3ffe:30:30:5::153 G2
```

Related commands

ipv6 pim rp-candidate

ipv6 pim rp-register-kat

ipv6 pim rp-candidate

Overview Use this command to make the device an RP (Rendezvous Point) candidate, using the IPv6 address of the specified VLAN interface.

Use the **no** variant of this command to stop the device from being an RP candidate.

Syntax

```
ipv6 pim rp-candidate <interface> [priority <priority>|interval
<interval>|grouplist <accesslist>]
```

```
no ipv6 pim rp-candidate [<interface>]
```

Parameter	Description
<interface>	Specify a VLAN interface name.
<priority>	Specify the priority for the RP candidate in the range 0 to 255.
<interval>	Specify a candidate RP advertisement interval in the range 1 to 16383 (seconds).
<accesslist>	Specify a Standard or an Extended software IPv6 access list name. See the IPv6 Software Access Control List (ACL) Commands chapter for supported IPv6 ACLs.

Default The priority value for a candidate RP is 192 by default until specified using the **priority** parameter.

Mode Global Configuration

Usage notes Note that issuing the command **ipv6 pim rp-candidate** *<interface>* without optional **priority**, **interval**, or **grouplist** parameters will configure the candidate RP with a priority value of 192.

Examples To specify a priority of 3, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim rp-candidate vlan2 priority 3
```

To use the ACL named G2 to specify the group prefixes that are advertised in association with the RP address, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard G2 permit
2001:db8::/128
awplus(config)# ipv6 pim rp-candidate vlan2 group-list G2
```

To stop the device from being an RP candidate on vlan2 , use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim rp-candidate vlan2
```

Related commands

ipv6 pim rp-address

ipv6 pim rp-register-kat

ipv6 pim rp embedded

Overview Use this command to configure and enable embedded RP (Rendezvous Point) in PIM-SMv6.

This command only applies to the embedded RP group range **ff7x::/12** and **fffx::/12**.

Use the **no** variant of this command to disable embedded RP support. Since embedded RP support is enabled by default, use the **no** variant of this command to disable the default.

Syntax

```
ipv6 pim rp embedded
no ipv6 pim rp embedded
```

Mode Global Configuration

Default Embedded RP is enabled by default in the AlliedWare Plus implementation of PIM-SMv6.

Examples The following example re-enables embedded RP support, the default state in PIM-SMv6:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim rp embedded
```

The following example disables embedded RP support, which is enabled by default in PIM-SMv6:

```
awplus# configure terminal
awplus(config)# no ipv6 pim rp embedded
```

ipv6 pim rp-register-kat

Overview Use this command to configure the Keep Alive Time (KAT) for (S,G) states at the RP (Rendezvous Point) to monitor PIM-SMv6 Register packets.

Use the **no** variant of this command to return the PIM-SMv6 KAT timer to its default value of 210 seconds.

Syntax

```
ipv6 pim rp-register-kat <1-65535>
no ipv6 pim rp-register-kat
```

Parameter	Description
<1-65536>	Specify the KAT timer in seconds. The default value is 210 seconds.

Mode Global Configuration

Default The default PIM-SMv6 KAT timer value is 210 seconds.

Examples

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim rp-register-kat 3454
awplus# configure terminal
awplus(config)# no ipv6 pim rp-register-kat
```

Related commands ipv6 pim rp-address

ipv6 pim rp-candidate

ipv6 pim sparse-mode

Overview Use this command to enable PIM-SMv6 on a VLAN interface.

Use the **no** variant of this command to disable PIM-SMv6 on a VLAN interface.

Syntax

```
ipv6 pim sparse-mode
no ipv6 pim sparse-mode
```

Mode Interface Configuration for a VLAN interface.

Examples

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim sparse-mode
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 pim sparse-mode
```

ipv6 pim sparse-mode passive

Overview Use this command to enable and disable PIM-SMv6 passive mode operation for local members on a VLAN interface.

Use the **no** variant of this command to disable PIM-SMv6 passive mode operation for local members on a VLAN interface.

Syntax
```
ipv6 pim sparse-mode passive
no ipv6 pim sparse-mode passive
```

Mode Interface Configuration for a VLAN interface.

Usage Passive mode essentially stops PIM-SMv6 transactions on the interface, allowing only the MLD mechanism to be active.

Examples
```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim sparse-mode passive
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 pim sparse-mode passive
```

ipv6 pim spt-threshold

Overview This command turns on the ability for the last-hop PIM-SMv6 router to switch to SPT (shortest-path tree).

The **no** variant of this command turns off the ability for the last-hop PIM-SMv6 router to switch to SPT.

NOTE: *The switching to SPT happens either at the receiving of the first data packet, or not at all; it is not rate-based.*

Syntax

```
ipv6 pim spt-threshold
no ipv6 pim spt-threshold
```

Mode Global Configuration

Examples To enable the last-hop PIM-SMv6 router to switch to SPT, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim spt-threshold
```

To stop the last-hop PIM-SMv6 router from being able to switch to SPT, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim spt-threshold
```

Related commands ipv6 pim spt-threshold group-list

ipv6 pim spt-threshold group-list

Overview Use this command to turn on/off the ability for the last-hop PIM-SMv6 router to switch to SPT (shortest-path tree) for multicast group addresses as specified by the given software IPv6 access-list.

Use the **no** variant of this command to turn off switching to the SPT.

NOTE: *The switching to SPT happens either at the receiving of the first data packet, or not at all; it is not rate-based.*

Syntax

```
ipv6 pim spt-threshold group-list <IPv6-access-list>
no ipv6 pim spt-threshold group-list <IPv6-access-list>
```

Parameter	Description
<IPv6-access-list>	Specify a Standard or an Extended software IPv6 access-list name. See the IPv6 Software Access Control List (ACL) Commands chapter for supported IPv6 ACLs.

Mode Global Configuration

Examples To enable the last-hop PIM-SMv6 router to switch to SPT for groups specified by the ACL named G1, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim spt-threshold group-list G1
awplus(config)# ipv6 access-list standard G1 permit
2001:db8::/128
```

To stop the last-hop PIM-SMv6 router from being able to switch to SPT for groups specified by the ACL named G1, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim spt-threshold group-list G1
```

Related commands ipv6 pim spt-threshold

ipv6 pim ssm

Overview Use this command to define the Source Specific Multicast (SSM) range of IPv6 multicast addresses. PIM-SMv6 routers will only install (S,G) entries for multicast groups (addresses) residing in the SSM range.

Use the **no** variant of this command to disable the SSM range.

Syntax

```
ipv6 pim ssm [default|range <named-access-list>]
no ipv6 pim ssm
```

Parameter	Description
`default`	Named Standard Access List. Use FF3x::/32 group range for SSM.
`range`	Specify an ACL for group range to be used for SSM.
`<named-access-list>`	Specify a named standard access list.

Default By default, the command is disabled.

Mode Global Configuration

Usage Any (*,G) or (S,G,rpt) joins received for multicast groups (addresses) within the range, are not installed in PIM-SMv6 mroute table.

Examples The following example shows how to configure SSM service for the IPv6 address range defined by IPv6 access list IPv6-PIM-SSM-RANGE:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard IPv6-PIM-SSM-RANGE
permit ff3e::/32
awplus(config)# ipv6 pim ssm range IPv6-PIM-SSM-RANGE
```

The following commands show how to set PIM-SSM as default:

```
awplus# configure terminal
awplus(config)# ipv6 pim ssm default
```

The following commands show how to disable PIM-SSM:

```
awplus# configure terminal
awplus(config)# no ipv6 pim ssm
```

ipv6 pim unicast-bsm

Overview Use this command to enable support for the sending and receiving of unicast Boot Strap Messages (BSM) on a VLAN interface.

Use the **no** variant of this command to disable the sending and receiving of unicast BSM on a VLAN interface.

Syntax
```
ipv6 pim unicast-bsm
no ipv6 pim unicast-bsm
```

Mode Interface Configuration for a VLAN interface.

Default Unicast BSM is disabled by default on an interface.

Usage This command provides backward compatibility with older versions of the Boot Strap Router (BSR) specification, which directs unicast BSM to refresh the state of new or restarting neighbors. The current BSR specification defines a No Forward BSM to achieve the same result.

Examples
```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim unicast-bsm
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 pim unicast-bsm
```

service pim6

Overview Use this command to enable IPv6 PIM sparse mode services.

Use the **no** version of the command to disable unused IPv6 PIM sparse mode services.

Syntax

```
service pim6
no service pim6
```

Default Enabled

Mode Global Configuration

Usage notes Sometimes it may be desirable to disable unused services, in order to reduce memory use.

Disabling the PIM services will only take effect after you save the configuration and restart the device.

Example To disable the IPv6 PIM sparse mode service, use the commands:

```
awplus# configure terminal
awplus(config)# no service pim6
```

Output Figure 36-2: Example output from **no service pim6**

```
awplus(config)#no service pim6
% Save the config and restart the device for this change to take
effect
```

Command changes Version 5.5.0-0.1: command added

show debugging ipv6 pim sparse-mode

Overview Use this command to see what debugging is turned on for PIM-SMv6.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show debugging ipv6 pim sparse-mode
```

Mode User Exec and Privileged Exec

Example To display PIM-SMv6 debugging settings, use the command:

```
awplus# show debugging ipv6 pim sparse-mode
```

Figure 36-3: Example output from the **show debugging ipv6 pim sparse-mode** command

```
awplus#show debugging ipv6 pim sparse-mode
Debugging status:
  PIM event debugging is on
  PIM MFC debugging is on
  PIM state debugging is on
  PIM packet debugging is on
  PIM Hello HT timer debugging is on
  PIM Hello NLT timer debugging is on
  PIM Hello THT timer debugging is on
  PIM Join/Prune JT timer debugging is on
  PIM Join/Prune ET timer debugging is on
  PIM Join/Prune PPT timer debugging is on
  PIM Join/Prune KAT timer debugging is on
  PIM Join/Prune OT timer debugging is on
  PIM Assert AT timer debugging is on
  PIM Register RST timer debugging is on
  PIM Bootstrap BST timer debugging is on
  PIM Bootstrap CRP timer debugging is on
```

Related commands debug ipv6 pim sparse-mode

undebug ipv6 pim sparse-mode

show ipv6 pim sparse-mode bsr-router

Overview Use this command to show the PIM-SMv6 Bootstrap Router (BSR) IPv6 address.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 pim sparse-mode bsr-router
```

Mode User Exec and Privileged Exec

Example To display the BSR IPv6 address, use the command:

```
awplus# show ipv6 pim sparse-mode bsr-router
```

Output Figure 36-4: Example output from the **show ipv6 pim sparse-mode bsr-router** command

```
awplus#show ipv6 pim sparse-mode bsr-router
PIM6v2 Bootstrap information
  BSR address: 2001:203::213 (?)
  Uptime:      00:36:25, BSR Priority: 64, Hash mask length: 126
  Expires:     00:01:46
  Role: Candidate BSR
  State: Candidate BSR

  Candidate RP: 2001:5::211(vlan5)
    Advertisement interval 60 seconds
    Next C-RP advertisement in 00:00:43
```

Related commands

show ipv6 pim sparse-mode rp mapping

show ipv6 pim sparse-mode neighbor

show ipv6 pim sparse-mode interface

Overview Use this command to show PIM-SMv6 interface information. Note that you can specify an individual VLAN interface with the optional parameter. Alternatively, you can display PIM-SMv6 interface information for all interfaces if you omit the optional 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 pim sparse-mode interface
```

Mode User Exec and Privileged Exec

Examples To display information about all PIM-SMv6 interfaces, use the command:

```
awplus# show ipv6 pim sparse-mode interface
```

```
awplus#show ipv6 pim sparse-mode interface
Interface VIFindex Ver/   Nbr    DR
                   Mode   Count  Priority
vlan2     0        v2/S   2      1
    Address       : fe80::207:e9ff:fe02:81d
    Global Address: 3ffe:192:168:1::53
    DR            : fe80::20e:cff:fe01:facc
vlan3     2        v2/S   2      1
    Address       : fe80::207:e9ff:fe02:21a2
    Global Address: 3ffe:192:168:10::53
    DR            : this system
```

Table 1: Parameters in the output from the **show ipv6 pim sparse-mode interface** command

Parameters	Description
Address	Primary PIM-SMv6 address.
Interface	Name of the PIM-SMv6 interface.
VIF Index	The Virtual Interface index of the VLAN.
Ver/Mode	PIMv6 version/Sparse mode.
Nbr Count	Neighbor count of the PIM-SMv6 interface.
DR Priority	Designated Router priority.
DR	The IPv6 address of the Designated Router.

Related commands

ipv6 pim sparse-mode

show ipv6 pim sparse-mode rp mapping

show ipv6 pim sparse-mode neighbor

show ipv6 pim sparse-mode interface detail

Overview Use this command to show detailed PIM-SMv6 information for all PIM-SMv6 configured interfaces.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 pim sparse-mode interface detail
```

Mode User Exec and Privileged Exec

Example To show detailed PIM-SMv6 information for all PIM-SMv6 configured interfaces, use the command:

```
awplus# show ipv6 pim sparse-mode interface detail
```

Output Figure 36-5: Example output from the **show ipv6 pim sparse-mode interface detail** command

```
awplus#show ipv6 pim sparse-mode interface detail
vlan2 (vif 0)
  Address fe80::207:e9ff:fe02:81d, DR fe80::20e:cff:fe01:facc
  Hello period 30 seconds, Next Hello in 21 seconds
  Triggered Hello period 5 seconds
  Secondary addresses:
   3ffe:192:168:1::53
  Neighbors:
   fe80::202:b3ff:fed4:69fe
   fe80::20e:cff:fe01:facc

vlan3 (vif 2):
  Address fe80::207:e9ff:fe02:21a2, DR fe80::207:e9ff:fe02:21a2
  Hello period 30 seconds, Next Hello in 20 seconds
  Triggered Hello period 5 seconds
  Secondary addresses:
   3ffe:192:168:10::53
  Neighbors:
```

show ipv6 pim sparse-mode local-members

Overview Use this command to show detailed local member information on a VLAN interface configured for PIM-SMv6. If you do not specify a VLAN interface then detailed local member information is shown for all VLAN interfaces configured for PIM-SMv6.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 pim sparse-mode local-members [<interface>]
```

Parameter	Description
<interface>	Optional Specify the interface. For instance, VLAN interface `vlan2`.

Mode User Exec and Privileged Exec

Example To show detailed PIM-SMv6 information for all PIM-SMv6 configured VLAN interfaces, use the command:

```
awplus# show ipv6 pim sparse-mode local-members
```

Output Figure 36-6: Example output from the **show ipv6 pim sparse-mode local-members** command

```
awplus#show ipv6 pim sparse-mode local-members
PIM Local membership information

vlan1:

  (*, ff02::1:ff6b:4783) : Include

vlan203:

  (*, ff0e:1::4) : Include
```

Example To show detailed PIM-SMv6 information for the PIM-SMv6 configured interface vlan1, use the command:

```
awplus# show ipv6 pim sparse-mode local-members vlan1
```

Output Figure 36-7: Example output from the **show ipv6 pim sparse-mode local-members vlan1** command

```
awplus#show ipv6 pim sparse-mode local-members vlan1
PIM Local membership information

vlan1:

  (*, ff02::1:ff6b:4783) : Include
```

show ipv6 pim sparse-mode mroute

Overview This command displays the IPv6 multicast routing table, or the IPv6 multicast routing table based on the specified IPv6 address or addresses.

Two group IPv6 addresses cannot be entered simultaneously; two source IPv6 addresses cannot be entered simultaneously.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 pim sparse-mode mroute
show ipv6 pim sparse-mode mroute <group-IPv6-address>
show ipv6 pim sparse-mode mroute <source-IPv6-address>
show ipv6 pim sparse-mode mroute <group-IPv6-address>
<source-IPv6-address>
show ipv6 pim sparse-mode mroute <source-IPv6-address>
<group-IPv6-address>
show ipv6 pim sparse-mode mroute brief
```

Parameter	Description
<group-IPv6-address>	Group IPv6 address, entered in the form X:X::X:X. Based on the group and source IPv6 address, the output is the selected route if present in the multicast route tree.
<source-IPv6-address>	Source IPv6 address, entered in the form X:X::X:X. Based on the source and group IPv6 address, the output is the selected route if present in the multicast route tree.
`brief`	Brief display

Mode User Exec and Privileged Exec

Usage notes Note that when a feature license is enabled, the output for the show ipv6 pim sparse-mode mroute command will only show 100 interfaces because of the terminal display width limit. Use the show ipv6 pim sparse-mode mroute detail command to display detailed entries of the IPv6 multicast routing table.

Examples

```
awplus# show ipv6 pim sparse-mode mroute
awplus# show ipv6 pim sparse-mode mroute 2001:db8::
awplus# show ipv6 pim sparse-mode mroute 2001:db8:: 2002:db8::
awplus# show ipv6 pim sparse-mode mroute brief
```

Figure 36-8: Example output from the **show ipv6 pim sparse-mode mroute** command

```
awplus#show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0(*,G) Entries: 0
(S,G) Entries: 2
(S,G,rpt) Entries: 2
FCR Entries: 0(2001:db8:ffff::1, ff08::1)
RPF nbr: fe80::b:10:0:1
RPF idx: vlan10
SPT bit: 1
Upstream State: JOINED
 Local            0
 Joined           1
 Asserted Winner  0
 Asserted Loser   0
 Outgoing         1(2001:db8:ffff::1, ff08::1, rpt)
RP: ::
RPF nbr: fe80::b:10:0:1
RPF idx: vlan10
Upstream State: RPT NOT JOINED
 Local     0
 Pruned    0
 Outgoing  0(2001:db8:ffff::1, ff08::2)
RPF nbr: fe80::b:10:0:1
RPF idx: vlan10
SPT bit: 1
Upstream State: JOINED
 Local            0
 Joined           1
 Asserted Winner  0
 Asserted Loser   0
 Outgoing         1
```

Figure 36-9: Example output from the **show ipv6 pim sparse-mode mroute brief** command

```
awplus#show ipv6 pim sparse-mode mroute brief
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 2
(S,G,rpt) Entries: 2
FCR Entries: 0
```

show ipv6 pim sparse-mode mroute detail

Overview This command displays detailed entries of the IPv6 multicast routing table, or detailed entries of the IPv6 multicast routing table based on the specified IPv6 address or addresses.

Two group IPv6 addresses cannot be used simultaneously; two IPv6 source addresses cannot be used simultaneously.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 pim sparse-mode mroute
[<group-IPv6-address>|<source-IPv6-address>] detail
```

```
show ipv6 pim sparse-mode mroute [<group-IPv6-address>
<source-IPv6-address>] detail
```

```
show ipv6 pim sparse-mode mroute [<source-IPv6-address>
<group-IPv6-address>] detail
```

Parameter	Description
<group-IPv6-address>	Group IPv6 address, entered in the form X:X::X:X. Output is all multicast entries belonging to that group.
<source-IPv6-address>	Source IPv6 address, entered in the form X:X::X:X. Output is all multicast entries belonging to that source.
`detail`	Show detailed information.

Usage notes Based on the group and source IPv6 address, the output is the selected route if present in the multicast route tree.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ipv6 pim sparse-mode mroute detail
```

```
awplus# show ipv6 pim sparse-mode mroute 2001:db8:: detail
```

```
awplus# show ipv6 pim sparse-mode mroute 2001:db8:: 2002:db8::
detail
```

Figure 36-10: Example output from the **show ipv6 pim sparse-mode mroute detail** command

```
awplus#show ipv6 pim sparse-mode mroute detail
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, ff13::10) Uptime: 00:00:09
  RP: ::, RPF nbr: None, RPF idx: None
  Upstream:
   State: JOINED, SPT Switch: Enabled, JT: off
   Macro state: Join Desired,
  Downstream:
   vlan2:
     State: NO INFO, ET: off, PPT: off
     Assert State: NO INFO, AT: off
      Winner: ::, Metric: 42949672951, Pref: 42949672951, RPT bit: on
     Macro state: Could Assert, Assert Track
  Local Olist:
   vlan3
  FCR:
```

show ipv6 pim sparse-mode neighbor

Overview Use this command to show the PIM-SMv6 neighbor information.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 pim sparse-mode neighbor [<interface>]
[<IPv6-address>] [detail]
```

Parameter	Description
<interface>	Interface name (e.g. vlan2). Show neighbors on an interface.
<IPv6-address>	Show neighbors with a particular address on an interface. The IPv6 address entered in the form X:X::X:X.
detail	Show detailed information.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ipv6 pim sparse-mode neighbor
awplus# show ipv6 pim sparse-mode neighbor vlan5 detail
```

Figure 36-11: Example output from the **show ipv6 pim sparse-mode neighbor** command

```
awplus#show ipv6 pim sparse-mode neighbor
Neighbor Address                     Interface   Uptime/Expires      DR
                                                                        Pri/Mode
fe80::202:b3ff:fed4:69fe              vlan2       05:33:52/00:01:41 1 /
fe80::20e:cff:fe01:facc               vlan3       05:33:53/00:01:26 1 / DR
```

Figure 36-12: Example output from the **show ipv6 pim sparse-mode neighbor interface detail** command

```
awplus#show ipv6 pim sparse-mode neighbor detail
Nbr fe80::211:11ff:fe44:4cd8 (vlan1), DR
 Expires in 64 seconds, uptime 00:00:53
 Holdtime: 70 secs, T-bit: off, Lan delay: 1, Override interval: 3
 DR priority: 100, Gen ID: 1080091886,
 Secondary addresses:
  3ffe:10:10:10:3::180
```

show ipv6 pim sparse-mode nexthop

Overview Use this command to see the next hop information as used by PIM-SMv6.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 pim sparse-mode nexthop
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 pim sparse-mode nexthop
```

Figure 36-13: Example output from the **show ipv6 pim sparse-mode nexthop** command

```
awplus#show ipv6 pim sparse-mode nexthop
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination           Type  Nexthop Nexthop Nexthop  Nexthop Metric     Pref   Refcnt
                            Num     Addr    Ifindex  Name
_____________________________________________________________________________________
3ffe:10:10:5::153     .RS.  1       fe80::20e:cff:fe01:facc  2     30   110    1
```

Table 2: Parameters in output of the **show ipv6 pim sparse-mode nexthop** command

Parameter	Description
Destination	The destination address for which PIM-SMv6 requires next hop information.
Type	The type of destination, as indicated by the Flags description. N = New, R= RP, S = Source, U = Unreachable.
Nexthop Num	The number of next hops to the destination. PIM-SMv6 always uses only 1 next hop.
Nexthop Addr	The address of the primary next hop gateway.
Nexthop IfIndex	The interface on which the next hop gateway can be reached.
Nexthop Name	The name of next hop interface.
Metric	The metric of the route towards the destination.
Preference	The preference of the route towards destination.
Refcnt	Only used for debugging.

show ipv6 pim sparse-mode rp-hash

Overview Use this command to display the Rendezvous Point (RP) to be chosen based on the IPv6 group address selected.

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

Syntax

```
show ipv6 pim sparse-mode rp-hash <IPv6-group-addr>
```

Parameter	Description
<IPv6-group-addr>	The IPv6 group address used to find the RP, entered in the form X:X::X:X.

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 pim sparse-mode rp-hash ff04:10
```

Figure 36-14: Output from the **show ipv6 pim sparse-mode rp-hash** command:

```
awplus#show ipv6 pim sparse-mode rp-hash ff04::10
    RP: 3ffe:10:10:5::153
    Info source: 3ffe:10:10:5::153, via bootstrap
```

Related commands show ipv6 pim sparse-mode rp mapping

show ipv6 pim sparse-mode rp mapping

Overview Use this command to show group-to-RP (Rendezvous Point) mappings, and the RP set.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 pim sparse-mode rp mapping
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 pim sparse-mode rp mapping
```

Figure 36-15: Output from the **show ipv6 pim sparse-mode rp mapping** command

```
awplus#show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): ff00::/8
  RP: 3ffe:10:10:5::153
    Info source: 3ffe:10:10:5::153, via bootstrap, priority 192
         Uptime: 05:36:40
```

Related commands show ipv6 pim sparse-mode rp-hash

show ipv6 pim sparse-mode rp nexthop

Overview Use this command to display the RP (Rendezvous Point) next hop information used by PIM-SMv6.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 pim sparse-mode rp nexthop <RP-group-addr>
```

Parameter	Description
<RP-group-addr>	Specify the RP group address used to display next hop RP information, entered in the form X:X::X:X.

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 pim sparse-mode rp nexthop 3ffe:10:10:5::153
```

Figure 36-16: Example output from the **show ipv6 pim sparse-mode rp nexthop** command

```
awplus#show ipv6 pim sparse-mode rp nexthop 3ffe:10:10:5::153
Flags: N = New, R = RP, S = Source, U = Unreachable
Destination           Type  Nexthop Nexthop Nexthop  Nexthop Metric     Pref   Refcnt
                            Num     Addr    Ifindex  Name
_____________________________________________________________________________________
3ffe:10:10:5::153     .RS.  1       fe80::20e:cff:fe01:facc  2     30   110    1
```

Table 3: Parameters in output of the **show ipv6 pim sparse-mode rp nexthop** command

Parameter	Description
`Destination`	The destination address for which PIM-SMv6 requires next hop information.
`Type`	The type of destination, as indicated by the Flags description. N = New, R= RP, S = Source, U = Unreachable.
`Nexthop Num`	The number of next hops to the destination. PIM-SMv6 always uses only 1 next hop.
`Nexthop Addr`	The address of the primary next hop gateway.
`Nexthop IfIndex`	The interface on which the next hop gateway can be reached.
`Nexthop Name`	The name of next hop interface.

Table 3: Parameters in output of the **show ipv6 pim sparse-mode rp nexthop** command (cont.)

Parameter	Description
`Metric`	The metric of the route towards the destination.
`Preference`	The preference of the route towards destination.
`Refcnt`	Only used for debugging.

undebug all ipv6 pim sparse-mode

Overview Use this command to disable all PIM-SMv6 debugging.

Syntax
```
undebug all ipv6 pim sparse-mode
```

Mode Privileged Exec

Example
```
awplus# undebug all ipv6 pim sparse-mode
```

Related commands debug ipv6 pim sparse-mode

undebug ipv6 pim sparse-mode

Overview Use this command to deactivate PIM-SMv6 debugging. Note that this command is an alias of the no variant of the debug ipv6 pim sparse-mode command.

Syntax

```
undebug ipv6 pim sparse-mode [all] [events] [mfc] [mib]
[nexthop] [nsm] [state] [timer]
```

Parameter	Description
`all`	Deactivates all PIM-SMv6 debugging.
`events`	Deactivates debug printing of PIM-SMv6 events.
`mfc`	Deactivates debug printing of MFC (Multicast Forwarding Cache).
`mib`	Deactivates debug printing of PIM-SMv6 MIBs.
`nexthop`	Deactivates debug printing of PIM-SMv6 next hop communications.
`nsm`	Deactivates debugging of PIM-SMv6 NSM (Network Services Module) communications.
`state`	Deactivates debug printing of state transition on all PIM-SMv6 FSMs.
`timer`	Deactivates debug printing of PIM-SMv6 timers.

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# undebug ipv6 pim sparse-mode all
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# undebug ipv6 pim sparse-mode events
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# undebug ipv6 pim sparse-mode nexthop
```

Validation Output

Figure 36-17: Example output from the **show debugging ipv6 pim sparse-mode** command after issuing the **undebug ipv6 pim sparse-mode all** command

```
awplus#undebug ipv6 pim sparse-mode all
awplus#show debugging ipv6 pim sparse-mode
PIM-SMv6 debugging status:
  PIM event debugging is off
  PIM MFC debugging is off
  PIM state debugging is off
  PIM packet debugging is off
  PIM Hello HT timer debugging is off
  PIM Hello NLT timer debugging is off
  PIM Hello THT timer debugging is off
  PIM Join/Prune JT timer debugging is off
  PIM Join/Prune ET timer debugging is off
  PIM Join/Prune PPT timer debugging is off
  PIM Join/Prune KAT timer debugging is off
  PIM Join/Prune OT timer debugging is off
  PIM Assert AT timer debugging is off
  PIM Register RST timer debugging is off
  PIM Bootstrap BST timer debugging is off
  PIM Bootstrap CRP timer debugging is off
  PIM mib debugging is off
  PIM nsm debugging is off
  PIM nexthop debugging is off
```

Related commands

debug ipv6 pim sparse-mode

show debugging ipv6 pim sparse-mode

undebug all ipv6 pim sparse-mode

37 PIM-DM Commands

Introduction

Overview This chapter provides an alphabetical reference of PIM-DM commands. For commands common to PIM-SM and PIM-DM, see Multicast Commands.

Command List

- "debug pim dense-mode all" on page 1875
- "debug pim dense-mode context" on page 1876
- "debug pim dense-mode decode" on page 1877
- "debug pim dense-mode encode" on page 1878
- "debug pim dense-mode fsm" on page 1879
- "debug pim dense-mode mrt" on page 1880
- "debug pim dense-mode nexthop" on page 1881
- "debug pim dense-mode nsm" on page 1882
- "debug pim dense-mode vif" on page 1883
- "ip pim dense-mode" on page 1884
- "ip pim dense-mode passive" on page 1885
- "ip pim dense-mode wrong-vif-suppression" on page 1886
- "ip pim ext-srcs-directly-connected" on page 1887
- "ip pim hello-holdtime (PIM-DM)" on page 1888
- "ip pim hello-interval (PIM-DM)" on page 1889
- "ip pim max-graft-retries" on page 1890
- "ip pim neighbor-filter (PIM-DM)" on page 1892
- "ip pim propagation-delay" on page 1893
- "ip pim state-refresh origination-interval" on page 1894
- "service pdm" on page 1895

- "show debugging pim dense-mode" on page 1896
- "show ip pim dense-mode interface" on page 1897
- "show ip pim dense-mode interface detail" on page 1899
- "show ip pim dense-mode mroute" on page 1900
- "show ip pim dense-mode neighbor" on page 1901
- "show ip pim dense-mode neighbor detail" on page 1902
- "show ip pim dense-mode nexthop" on page 1903
- "undebug all pim dense-mode" on page 1904

debug pim dense-mode all

Overview This command enables PIM-DM debugging.

The **no** variant of this command disables PIM-DM debugging.

Syntax

```
debug pim dense-mode all
no debug pim dense-mode all
```

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# debug pim dense-mode all
```

Output Figure 37-1: Example output from the **debug pim dense-mode all** command

```
PIM event debugging is on

PIM MFC debugging is on

PIM state debugging is on

PIM packet debugging is on

PIM incoming packet debugging is on

PIM outgoing packet debugging is on
```

Validation Commands show debugging pim dense-mode

Related commands debug pim dense-mode context

debug pim dense-mode decode

debug pim dense-mode encode

debug pim dense-mode fsm

debug pim dense-mode mrt

debug pim dense-mode nexthop

debug pim dense-mode nsm

debug pim dense-mode vif

debug pim dense-mode context

Overview This command enables debugging of general configuration context.

The **no** variant of this command disables debugging of general configuration context.

Syntax

```
debug pim dense-mode context
no debug pim dense-mode context
```

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# debug pim dense-mode context
```

Related commands

debug pim dense-mode all

debug pim dense-mode decode

debug pim dense-mode encode

debug pim dense-mode fsm

debug pim dense-mode mrt

debug pim dense-mode nexthop

debug pim dense-mode nsm

debug pim dense-mode vif

debug pim dense-mode decode

Overview This command enables debugging of the PIM-DM message decoder.

The **no** variant of this command disables debugging of the PIM-DM message decoder.

Syntax

```
debug pim dense-mode decode
no debug pim dense-mode decode
```

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# debug pim dense-mode decoder
```

Related commands

debug pim dense-mode all

debug pim dense-mode context

debug pim dense-mode encode

debug pim dense-mode fsm

debug pim dense-mode mrt

debug pim dense-mode nexthop

debug pim dense-mode nsm

debug pim dense-mode vif

debug pim dense-mode encode

Overview This command enables debugging of the PIM-DM message encoder.

The **no** variant of this command disables debugging of the PIM-DM message encoder.

Syntax

```
debug pim dense-mode encode
no debug pim dense-mode encode
```

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# debug pim dense-mode encoder
```

Related commands

debug pim dense-mode all

debug pim dense-mode context

debug pim dense-mode decode

debug pim dense-mode fsm

debug pim dense-mode mrt

debug pim dense-mode nexthop

debug pim dense-mode nsm

debug pim dense-mode vif

debug pim dense-mode fsm

Overview This command enables debugging of Finite-State Machine (FSM) specific information of all Multicast Routing Table (MRT) and MRT Virtual Multicast Interface (MRT-VIF) entries.

The **no** variant of this command disables debugging of Finite-State Machine (FSM) specific information of all Multicast Routing Table (MRT) and MRT Virtual Multicast Interface (MRT-VIF) entries.

Syntax

```
debug pim dense-mode fsm
no debug pim dense-mode fsm
```

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# debug pim dense-mode fsm
```

Related commands

debug pim dense-mode all

debug pim dense-mode context

debug pim dense-mode decode

debug pim dense-mode encode

debug pim dense-mode mrt

debug pim dense-mode nexthop

debug pim dense-mode nsm

debug pim dense-mode vif

debug pim dense-mode mrt

Overview This command enables debugging of MRT and MRT-VIF entry handling (for example, creation and deletion of).

The **no** variant of this command disables debugging of MRT and MRT-VIF entry handling.

Syntax

```
debug pim dense-mode mrt
no debug pim dense-mode mrt
```

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# debug pim dense-mode mrt
```

Related commands

debug pim dense-mode all

debug pim dense-mode context

debug pim dense-mode decode

debug pim dense-mode encode

debug pim dense-mode fsm

debug pim dense-mode nexthop

debug pim dense-mode nsm

debug pim dense-mode vif

debug pim dense-mode nexthop

Overview This command enables debugging of Reverse Path Forwarding (RPF) neighbor next hop cache handling.

The **no** variant of this command disables debugging of Reverse Path Forwarding (RPF) neighbor next hop cache handling.

Syntax

```
debug pim dense-mode nexthop
no debug pim dense-mode nexthop
```

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# debug pim dense-mode nexthop
```

Related commands

debug pim dense-mode all

debug pim dense-mode context

debug pim dense-mode decode

debug pim dense-mode encode

debug pim dense-mode fsm

debug pim dense-mode mrt

debug pim dense-mode nsm

debug pim dense-mode vif

debug pim dense-mode nsm

Overview This command enables debugging of PIM-DM interface with NSM.

The **no** variant of this command disables debugging of PIM-DM interface with NSM.

Syntax

```
debug pim dense-mode nsm
no debug pim dense-mode nsm
```

Mode Privileged Exec and Global Configuration

Example

```
awplus# configure terminal
awplus(config)# debug pim dense-mode nsm
```

Related commands

debug pim dense-mode all

debug pim dense-mode context

debug pim dense-mode decode

debug pim dense-mode encode

debug pim dense-mode fsm

debug pim dense-mode mrt

debug pim dense-mode nexthop

debug pim dense-mode vif

debug pim dense-mode vif

Overview This command enables debugging of VIF handling.

The **no** variant of this command disables debugging of VIF handling.

Syntax
```
debug pim dense-mode vif
no debug pim dense-mode vif
```

Mode Privileged Exec and Global Configuration

Example
```
awplus# configure terminal
awplus(config)# debug pim dense-mode vif
```

Related commands
- debug pim dense-mode all
- debug pim dense-mode context
- debug pim dense-mode decode
- debug pim dense-mode encode
- debug pim dense-mode fsm
- debug pim dense-mode mrt
- debug pim dense-mode nexthop
- debug pim dense-mode nsm

ip pim dense-mode

Overview This command enables or disables PIM-DM operation from Interface mode on the current VLAN interface. This command also disables passive mode on the VLAN interface if passive mode has been enabled using an ip pim dense-mode passive command.

The **no** variant of this command disables all PIM-DM activities on the interface.

Syntax
```
ip pim dense-mode
no ip pim dense-mode
```

Mode Interface Configuration for a VLAN interface.

Example
```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim dense-mode
```

ip pim dense-mode passive

Overview This command enables PIM-DM passive mode operation from Interface mode on the current VLAN interface.

The **no** variant of this command disables passive mode.

Syntax

```
ip pim dense-mode passive
no ip pim dense-mode passive
```

Mode Interface Configuration for a VLAN interface.

Usage Configuring a VLAN interface as a passive PIM-DM interface indicates that the VLAN interface is connected to a stub network (i.e. a network that does not contain any PIM Routers). So, multicast streams that arrive on other PIM-DM interfaces can be routed to hosts on the passive PIM-DM interface, but no PIM neighbor relationships will be formed on the passive PIM-DM interface.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim dense-mode passive
```

ip pim dense-mode wrong-vif-suppression

Overview Use this command to permit or block packets that arrive on the wrong VLAN Interface (VIF) for PIM dense-mode.

Use the **no** variant of this command to disable dense-mode wrong VIF suppression

Syntax

```
ip pim dense-mode wrong-vif-suppression
no ip pim dense-mode wrong-vif-suppression
```

Default Disabled.

Mode Global Configuration

Usage notes This command enables wrong VIF suppression for PIM dense-mode. Wrong VIF suppression prevents multicast packets received on the wrong upstream interface from being copied to the CPU.

Examples To enable wrong VIF suppression, use the commands:

```
awplus# configure terminal
awplus(config)# ip pim dense-mode wrong-vif-suppression
```

To disable wrong VIF suppression, use the commands:

```
awplus# configure terminal
awplus(config)# no ip pim dense-mode wrong-vif-suppression
```

Command changes Version 5.4.8-2.3: command added.

ip pim ext-srcs-directly-connected

Overview Use this command to configure PIM to treat all source traffic arriving on the interface as though it was sent from a host directly connected to the interface.

Use the **no** variant of this command to configure PIM to treat only directly connected sources as directly connected.

Syntax

```
ip pim ext-srcs-directly-connected
no ip pim ext-srcs-directly-connected
```

Default The **no** variant of this command is the default behavior.

Mode Interface Configuration for a VLAN interface.

Example To configure PIM to treat all sources as directly connected for VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim ext-srcs-directly-connected
```

To configure PIM to treat only directly connected sources as directly connected for VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip pim ext-srcs-directly-connected
```

ip pim hello-holdtime (PIM-DM)

Overview This command configures a **hello-holdtime**. The PIM **hello-holdtime** on a VLAN interface is the period which the router will wait to receive a hello from neighbors on that interface. If the router does not receive a hello from a given neighbor within that period, then it will decide that the neighbor is no longer an active PIM Router, and will terminate the neighbor relationship.

You cannot configure a **hello-holdtime** value that is less than the current **hello-interval**. Each time the **hello-interval** is updated, the **hello-holdtime** is also updated, according to the following rules:

- If the **hello-holdtime** is not configured; or if the hello holdtime is configured and less than the current **hello-interval** value, it is modified to 3.5 times the **hello-interval** value.
- Otherwise, it retains the configured value.

Use the **no** variant of this command to return the hello-holdtime value to its default of 3.5 times the current hello-interval value.

Syntax

```
ip pim hello-holdtime <holdtime>
no ip pim hello-holdtime
```

Parameter	Description
<holdtime>	<1-65535> The holdtime value in seconds (no fractional seconds are accepted).

Mode Interface Configuration for a VLAN interface.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim hello-holdtime 123
```

ip pim hello-interval (PIM-DM)

Overview This command configures a PIM **hello-interval** value. The PIM **hello-interval** on a VLAN interface is the period at which the router will transmit PIM hello messages on that interface.

When the **hello-interval** is configured, and the **hello-holdtime** is not configured, or when the configured **hello-holdtime** value is less than the new **hello-interval** value; the **hello-holdtime** value is modified to 3.5 times the **hello-interval** value. Otherwise, the **hello-holdtime** value is the configured value. The default is 30 seconds.

Use the **no** variant of this command to reset the **hello-interval** to the default.

Syntax

```
ip pim hello-interval <interval>
no ip pim hello-interval
```

Parameter	Description
<interval>	*<1-65535>* The value in seconds (no fractional seconds accepted).

Mode Interface Configuration for a VLAN interface.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim hello-interval 123
```

ip pim max-graft-retries

Overview This command configures PIM-DM to send a limited number of Graft message retries, after which time the device will remove all information regarding the particular (Source, Group), or until the device receives an acknowledgment, whichever occurs first.

The **no** variant of this command configures PIM-DM to send Graft message retries until the device receives an acknowledgment, which is the default behavior.

Syntax

```
ip pim max-graft-retries <1-65535>
no pim max-graft-retries
```

Parameter	Description
`no`	Negate a command or set its defaults.
`ip`	Internet Protocol (IP).
`pim`	PIM Interface commands.
`max-graft-retries`	PIM Graft message retries.
<1-65535>	Graft message retries before ceasing Graft message retries.

Default By default, Graft retries are sent by PIM-DM until the device receives an acknowledgment.

Mode Interface Configuration for a VLAN interface.

Usage Graft messages are used to reduce the join latency when a previously pruned branch of the source tree must be grafted back, when a member joins the group after the PIM-DM device has sent a Prune message to prune unwanted traffic. Graft messages are the only PIM-DM messages that receive an acknowledgment.

If Graft messages were not used, then the member waiting for pruned off traffic would have to wait up to 3 minutes for the periodic re-flooding to occur to begin receiving multicast traffic again. By using Grafts, the Prune can be reversed much faster than waiting for periodic re-flooding to begin receiving multicast traffic again.

Examples To configure PIM-DM on the VLAN interface vlan2 to send a maximum of 10 Graft message retries, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim max-graft-retries 10
```

To configure PIM-DM on the VLAN interface vlan2 to send Graft message retries forever, which is the default behavior, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip pim max-graft-retries
```

Validation Commands

show ip mroute

show ip pim dense-mode mroute

show running-config

ip pim neighbor-filter (PIM-DM)

Overview Enables filtering of neighbors on the VLAN interface. When configuring a neighbor filter, PIM-DM will either not establish adjacency with the neighbor, or terminate adjacency with the existing neighbors if denied by the filtering access list.

Use the **no** variant of this command to disable this function.

Syntax

```
ip pim neighbor-filter [<number>|<accesslist>]
no ip pim neighbor-filter [<number>|<accesslist>]
```

Parameter	Description
<number>	*<1-99>* Standard IP access list number.
<accesslist>	IP access list name.

Default By default, there is no filtering.

Mode Interface Configuration for a VLAN interface.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim neighbor-filter 14
```

ip pim propagation-delay

Overview This command configures the PIM **propagation-delay** value. The PIM **propagation-delay** is the expected delay in the transfer of PIM messages across the VLAN interface that it is attached to.

Use the **no** variant of this command to return the **propagation-delay** to the default (1000 milliseconds).

Syntax

```
ip pim propagation-delay <delay>
no ip pim propagation-delay
```

Parameter	Description
<delay>	*<1000-5000>* The value in milliseconds. The default is 1000 milliseconds.

Default The propagation-delay is set to 1000 milliseconds by default.

Mode Interface Configuration for a VLAN interface.

Examples

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim propagation-delay 2000
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip pim propagation-delay
```

ip pim state-refresh origination-interval

Overview This command configures a PIM **state-refresh origination-interval** value. The origination interval is the number of seconds between PIM state refresh control messages. The default is 60 seconds.

Use the **no** variant of this command to return the origination interval to the default.

Syntax

```
ip pim state-refresh origination-interval <interval>
no ip pim state-refresh origination-interval
```

Parameter	Description
<interval>	*<1-100>* The integer value in seconds (no fractional seconds accepted). The default **state-refresh origination-interval** value is 60.

Default The state-refresh origination-interval is set to 60 seconds by default, and is reset using negation.

Mode Interface Configuration for a VLAN interface.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim state-refresh origination-interval 65
```

service pdm

Overview Use this command to enable PIM dense mode services.

Use the **no** version of the command to disable unused PIM dense mode services.

Syntax

```
service pdm
no service pdm
```

Default Enabled

Mode Global Configuration

Usage notes Sometimes it may be desirable to disable unused services, in order to reduce memory use.

Disabling the PIM services will only take effect after you save the configuration and restart the device.

Example To disable the PIM dense mode service, use the commands:

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

Output Figure 37-2: Example output from **no service pdm**

```
awplus(config)#no service pdm
% Save the config and restart the device for this change to take
effect
```

Command changes Version 5.5.0-0.1: command added

show debugging pim dense-mode

Overview This command displays the status of the debugging of the system.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show debugging pim dense-mode
```

Mode User Exec and Privileged Exec

Output Figure 37-3: Example output from the show debugging pim dense-mode command

```
PIM-DM Debugging status:
  PIM-DM Decoder debugging is off
  PIM-DM Encoder debugging is off
  PIM-DM FSM debugging is off
  PIM-DM MRT debugging is off
  PIM-DM NHOP debugging is off
  PIM-DM NSM debugging is off
  PIM-DM VIF debugging is off
```

Related commands debug pim dense-mode all

show ip pim dense-mode interface

Overview This command displays the PIM-DM interface information.

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

Syntax

```
show ip pim dense-mode interface
```

Mode User Exec and Privileged Exec

Example To display information about the PIM-DM interfaces, use the command:

```
awplus# show ip pim dense-mode interface
```

Output

```
Total configured interfaces: 24   Maximum allowed: 32
Total active interfaces:     22

Address          Interface VIFIndex Ver/   Nbr
                                    Mode   Count
192.168.1.53/24  vlan2     0        v2/D   2
192.168.2.1      vlan3     2        v2/D   0
...
Note that this screen has been edited to remove any additional
interfaces.
```

Table 1: Parameters in the output of the **show ip pim dense-mode interface** command

Parameter	Description
Total configured interfaces	The number of configured PIM Dense Mode interfaces.
Maximum allowed	The maximum number of PIM Dense Mode interfaces that can be configured.
Total active interfaces	The number of active PIM Dense Mode interfaces.
Address	Primary PIM-DM address.
Interface	Name of the PIM-DM interface.
VIF Index	The Virtual Interface index of the VLAN.
Ver/Mode	PIM version/Dense mode.
Nbr Count	Neighbor count of the PIM-DM interface.

Related commands

ip pim dense-mode

show ip pim dense-mode neighbor

show ip pim dense-mode interface detail

Overview This command displays detailed information on a PIM-DM interface.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ip pim dense-mode interface detail
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip pim dense-mode interface detail
```

Output Figure 37-4: Example output from the **show ip pim dense-mode interface detail** command

```
vlan2 (vif-id: 0):

 Address 192.168.1.53/24
  Hello period 30 seconds, Next Hello in 30 seconds

  Neighbors:
   192.168.1.152/32
   192.168.1.149/32
  vlan3 (vif-id: 2):
   Address 192.168.10.53/24
   Hello period 30 seconds, Next Hello in 8 seconds
   Neighbors: none
```

show ip pim dense-mode mroute

Overview This command displays the IP PIM-DM multicast routing table.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ip pim dense-mode mroute
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip pim dense-mode mroute
```

Output Figure 37-5: Example output from the **show ip pim dense-mode mroute** command

```
PIM-DM Multicast Routing Table

(192.168.10.52, 224.1.1.1)
 Source directly connected on vlan3
  State-Refresh Originator State: Originator
   Upstream IF: vlan3, State: Forwarding
   Downstream IF List:
   vlan2, in 'olist':
   Downstream State: NoInfo
   Assert State: NoInfo
```

show ip pim dense-mode neighbor

Overview This command displays PIM-DM neighbor information.

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

Syntax

```
show ip pim dense-mode neighbor
```

Mode User Exec and Privileged Exec

Usage notes The total number of PIM-DM neighbors is restricted to 500 PIM-DM neighbors.

When the 500 PIM-DM neighbor limit is reached, as a result of receiving hello packets from new PIM-DM neighbors, a log entry will be issued to the log file in the below format:

```
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
---------------------------------------------------------------
2008 Dec 10 00:58:39 user.err x908 PIM-DM[1150]: [VIF] Nbr
Create: Cannot create more than 500 neighbours - ignoring
neighbour 100.0.1.247/32 on vlan100
```

Example

```
awplus# show ip pim dense-mode neighbor
```

Output Figure 37-6: Example output from the **show ip pim dense-mode neighbor** command

```
Total number of neighbors: 500
Neighbor-Address  Interface            Uptime/Expires    Ver
192.168.1.152     vlan2                17:15:42/00:01:28 v2
192.168.1.149     vlan2                17:15:34/00:01:34 v2
```

show ip pim dense-mode neighbor detail

Overview This command displays detailed PIM-DM neighbor information.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ip pim dense-mode neighbor detail
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip pim dense-mode neighbor detail
```

Output Figure 37-7: Example output from the **show ip pim dense-mode neighbor detail** command

```
Neighbor 192.168.1.152 (vlan2)
Up since 17:16:20, Expires in 00:01:20
Neighbor 192.168.1.149 (vlan2)
Up since 17:16:12, Expires in 00:01:26
```

show ip pim dense-mode nexthop

Overview This command displays the next hop information as used by PIM-DM. In the context of PIM-DM, the term ' **next hop**' refers to the next hop router on the path back to the source address of a multicast stream.

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

Syntax
```
show ip pim dense-mode nexthop
```

Mode User Exec and Privileged Exec

Example
```
awplus# show ip pim dense-mode nexthop
```

Output Figure 37-8: Example output from the **show ip pim dense-mode neighbor nexthop** command

```
Destination      Nexthop    Nexthop     Nexthop       Metric Pref
                 Num        Addr        Interface
192.168.10.52    1          0.0.0.0     vlan2         3      1
```

Table 2: Parameters in the output of the **show ip pim dense-mode neighbor nexthop** command

Parameter	Description
Destination	Destination address for which PIM-DM requires next hop information.
Nexthop Num	Number of next hops to the destination. PIM can only use one next hop.
Nexthop Addr	Address of the current next hop gateway.
Nexthop Interface	Name of the next hop interface.
Metric	Metric of the route towards the destination.
Preference	Preference of the route towards the destination.

undebug all pim dense-mode

Overview Use this command from the Global Configuration mode to disable all PIM-DM debugging.

Syntax

```
undebug all pim dense-mode
```

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# undebug all pim dense-mode
```

Related commands

debug pim dense-mode all

debug pim dense-mode context

debug pim dense-mode decode

debug pim dense-mode encode

debug pim dense-mode fsm

debug pim dense-mode mrt

debug pim dense-mode nexthop

debug pim dense-mode nsm

debug pim dense-mode vif

Part 5: Access and Security

38 IPv4 Hardware Access Control List (ACL) Commands

Introduction

Overview This chapter provides an alphabetical reference of IPv4 Hardware Access Control List (ACL) commands. It contains detailed command information and command examples about IPv4 hardware ACLs, which you can apply directly to interfaces using the access-group command.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself.

Most ACL command titles include information in parentheses:

- When the command title ends with words in parentheses, these words indicate usage instead of keywords to enter into the CLI. For example, the title **access-list (numbered hardware ACL for ICMP)** indicates that the command is used to create an ACL with the syntax:

```
access-list <3000-3699> <action> icmp <source-ip> <dest-ip>
[icmp-type <number>] [vlan <1-4094>]
```

- When the command title is completely surrounded by parentheses, the title indicates the type of ACL filter instead of keywords to enter into the CLI. For example, the title **(named hardware ACL: ICMP entry)** represents a command with the syntax:

```
[<sequence-number>] <action> icmp <source-ip> <dest-ip>
[icmp-type <number>] [vlan <1-4094>]
```

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Sub-modes Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 38-1: IPv4 Hardware Access List Commands and Prompts

Command Name	Command Mode	Prompt
show interface access-group	Privileged Exec	awplus#
show access-group	Privileged Exec	awplus#
show access-list (IPv4 Hardware ACLs)	Privileged Exec	awplus#
show acl-group ip address	Privileged Exec	awplus#
show acl-group ip port	Privileged Exec	awplus#
show interface access-group	Privileged Exec	awplus#
access-list (numbered hardware ACL for IP packets)	Global Configuration	awplus(config)#
access-list (numbered hardware ACL for ICMP)	Global Configuration	awplus(config)#
access-list (numbered hardware ACL for IP protocols)	Global Configuration	awplus(config)#
access-list (numbered hardware ACL for TCP or UDP)	Global Configuration	awplus(config)#
access-list (numbered hardware ACL for MAC addresses)	Global Configuration	awplus(config)#
access-list hardware (named hardware ACL)	Global Configuration	awplus(config)#
acl-group ip address	Global Configuration	awplus(config)#
acl-group ip port	Global Configuration	awplus(config)#
(named hardware ACL entry for IP packets)	IPv4 Hardware ACL Configuration	awplus(config-ip-hw-acl)#
(named hardware ACL entry for ICMP)	IPv4 Hardware ACL Configuration	awplus(config-ip-hw-acl)#
(named hardware ACL entry for IP protocols)	IPv4 Hardware ACL Configuration	awplus(config-ip-hw-acl)#
(named hardware ACL entry for TCP or UDP)	IPv4 Hardware ACL Configuration	awplus(config-ip-hw-acl)#
(named hardware ACL entry for MAC addresses)	IPv4 Hardware ACL Configuration	awplus(config-ip-hw-acl)#
commit (IPv4)	IPv4 Hardware ACL Configuration	awplus(config-ip-hw-acl)#
ip (ip-host-group)	ACL Host Group Configuration	awplus(config-ip-host-group)#
(acl-group ip port range)	ACL Port Group Configuration	awplus(config-ip-port-group)#
access-group	Interface Configuration	awplus(config-if)#

References

For descriptions of ACLs, and further information about rules when applying them, see the ACL Feature Overview and Configuration Guide.

For more information on link aggregation see the following references:

- the Link Aggregation Feature Overview_and_Configuration_Guide.
- Link Aggregation Commands

Command List

- "access-group" on page 1909
- "access-list (numbered hardware ACL for ICMP)" on page 1911
- "access-list (numbered hardware ACL for IP packets)" on page 1915
- "access-list (numbered hardware ACL for IP protocols)" on page 1918
- "access-list (numbered hardware ACL for MAC addresses)" on page 1923
- "access-list (numbered hardware ACL for TCP or UDP)" on page 1926
- "access-list hardware (named hardware ACL)" on page 1930
- "acl-group ip address" on page 1932
- "acl-group ip port" on page 1933
- "(acl-group ip port range)" on page 1934
- "commit (IPv4)" on page 1936
- "ip (ip-host-group)" on page 1937
- "(named hardware ACL entry for ICMP)" on page 1939
- "(named hardware ACL entry for IP packets)" on page 1943
- "(named hardware ACL entry for IP protocols)" on page 1947
- "(named hardware ACL entry for MAC addresses)" on page 1952
- "(named hardware ACL entry for TCP or UDP)" on page 1955
- "show access-group" on page 1959
- "show access-list (IPv4 Hardware ACLs)" on page 1960
- "show acl-group ip address" on page 1962
- "show acl-group ip port" on page 1963
- "show interface access-group" on page 1964

access-group

Overview This command adds or removes a hardware-based access-list to or from a switch port interface or interfaces. The number of hardware numbered and named access-lists that can be added to a switch port interface is determined by the available memory in hardware-based packet classification tables.

This command works in Interface Configuration mode to apply hardware access-lists to selected switch port interfaces.

The **no** variant of this command removes the selected access-list from an interface.

Syntax

```
access-group
[<3000-3699>|<4000-4699>|<hardware-access-list-name>]
```

```
no access-group
[<3000-3699>|<4000-4699>|<hardware-access-list-name>]
```

Parameter	Description
<3000-3699>	Hardware IP access-list.
<4000-4699>	Hardware MAC access-list.
<hardware-access-list-name>	The hardware access-list name.

Mode Interface Configuration for a switch port interface or interfaces

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage notes First create an IP access-list that applies the appropriate permit/deny requirements with the access-list (numbered hardware ACL for IP packets) command, the access-list (numbered hardware ACL for MAC addresses) command or the access-list hardware (named hardware ACL) command. Then use this command to apply this hardware access- list to a specific port or port range. Note that this command will apply the access-list only to incoming data packets.

To apply ACLs to an LACP aggregated link, apply it to all the individual switch ports in the aggregated group. To apply ACLs to a static channel group, apply it to the static channel group itself. An ACL can even be applied to a static aggregated link that spans more than one switch instance (Link Aggregation Commands).

Note that you cannot apply software numbered ACLs to switch port interfaces with the access-group command. This command will only apply hardware ACLs.

NOTE: *Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples

To add the numbered hardware access-list 3005 to switch port interface port1.0.1, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# access-group 3005
```

To add the named hardware access-list "hw-acl" to switch port interface port1.0.2, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# access-group hw-acl
```

To apply an ACL to static channel group 2 containing switch port1.0.3 and port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3-port1.0.4
awplus(config-if)# static-channel-group 2
awplus(config)# interface sa2
awplus(config-if)# access-group 3000
```

Related commands

access-list hardware (named hardware ACL)

access-list (numbered hardware ACL for IP packets)

access-list (numbered hardware ACL for MAC addresses)

show interface access-group

access-list (numbered hardware ACL for ICMP)

Overview This command creates an access-list for use with hardware classification. The access-list will match on ICMP packets that have the specified source and destination IP addresses and, optionally, ICMP type. You can use the value **any** instead of source or destination address if an address does not matter.

Once you have configured the ACL, you can use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map.

The optional **vlan** parameter can be used to match tagged (802.1q) packets.

The **no** variant of this command removes the previously specified access-list.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
access-list <3000-3699> <action> icmp <source-ip> <dest-ip>
[icmp-type <number>] [vlan <1-4094>]

no access-list <3000-3699>
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Parameter	Description	
<3000-3699>	An ID number for this hardware IP access-list.	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
icmp	Match against ICMP packets	
<source-ip>	The source addresses to match against. You can specify a single host, a subnet, or all source addresses. The following are the valid formats for specifying the source:	
	any	Match any source IP address.
	host *<ip-addr>*	Match a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	Match any source IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> *<reverse-mask>*	Match any source IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<dest-ip>	The destination addresses to match against. You can specify a single host, a subnet, or all destination addresses. The following are the valid formats for specifying the destination:	
	any	Match any destination IP address.
	host *<ip-addr>*	Match a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	Match any destination IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> *<reverse-mask>*	Match any destination IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
icmp-type *<number>*	The type of ICMP message to match against, as defined in RFC792 and RFC950. Values include:	
	0	Echo replies.

Parameter	Description	
	3	Destination unreachable messages.
	4	Source quench messages.
	5	Redirect (change route) messages.
	8	Echo requests.
	11	Time exceeded messages.
	12	Parameter problem messages.
	13	Timestamp requests.
	14	Timestamp replies.
	15	Information requests.
	16	Information replies.
	17	Address mask requests.
	18	Address mask replies.
`vlan <1-4094>`	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Mode Global Configuration

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes This command creates an ACL for use with hardware classification. Once you have configured the ACL, use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map.

ACLs numbered in the range 3000-3699 match on packets that have the specified source and destination IP addresses.

ICMP ACLs will match any ICMP packet that has the specified source and destination IP addresses and ICMP type. The ICMP type is an optional parameter.

Examples To create an access-list that will permit ICMP packets with a source address of 192.168.1.0/24 with any destination address and an ICMP type of 5 enter the following commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit icmp 192.168.1.0/24 any
icmp-type 5
```

To destroy the access-list with an access-list identity of 3000 enter the following commands:

```
awplus# configure terminal
awplus(config)# no access-list 3000
```

Related commands access-group

match access-group

show running-config

show access-list (IPv4 Hardware ACLs)

access-list (numbered hardware ACL for IP packets)

Overview

This command creates an access-list for use with hardware classification. The access-list will match on packets that have the specified source and destination IP addresses. You can use the value **any** instead of source or destination address if an address does not matter.

Once you have configured the ACL, you can use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map.

The optional **vlan** parameter can be used to match tagged (802.1q) packets.

The **no** variant of this command removes the previously specified IP hardware access-list.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
access-list <3000-3699> <action> ip <source-ip> <dest-ip> [vlan <1-4094>]
no access-list <3000-3699>
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Table 38-2: IP and ICMP parameters in **access-list (hardware IP numbered)**

Parameter	Description	
<3000-3699>	An ID number for this hardware IP access-list.	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
ip	Match against IP packets	
<source-ip>	The source addresses to match against. You can specify a single host, a subnet, or all source addresses. The following are the valid formats for specifying the source:	
	any	Match any source IP address.
	host *<ip-addr>*	Match a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	Match any source IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> <reverse-mask>	Match any source IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<dest-ip>	The destination addresses to match against. You can specify a single host, a subnet, or all destination addresses. The following are the valid formats for specifying the destination:	
	any	Match any destination IP address.
	host *<ip-addr>*	Match a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	Match any destination IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> <reverse-mask>	Match any destination IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
vlan *<1-4094>*	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Mode Global Configuration

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes This command creates an ACL for use with hardware classification. Once you have configured the ACL, use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map.

ACLs numbered in the range 3000-3699 match on packets that have the specified source and destination IP addresses.

Examples To create an access-list that will permit IP packets with a source address of 192.168.1.1 and any destination address, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit ip 192.168.1.1/32 any
```

To destroy the access-list with an access-list identity of 3000 enter the following commands:

```
awplus# configure terminal
awplus(config)# no access-list 3000
```

Related commands access-group

match access-group

show running-config

show access-list (IPv4 Hardware ACLs)

access-list (numbered hardware ACL for IP protocols)

Overview This command creates an access-list for use with hardware classification. The access-list will match on packets that have the specified source and destination IP addresses and IP protocol number. You can use the value **any** instead of source or destination address if an address does not matter.

Once you have configured the ACL, you can use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map.

The optional **vlan** parameter can be used to match tagged (802.1q) packets.

The **no** variant of this command removes the previously specified IP hardware access-list.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
access-list <3000-3699> <action> proto <1-255> <source-ip>
<dest-ip> [vlan <1-4094>]

no access-list <3000-3699>
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Table 38-3: Parameters in **access-list (hardware IP numbered)**

Parameter	Description	
<3000-3699>	An ID number for this hardware IP access-list.	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
`proto` *<1-255>*	The IP protocol number to match against, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.	
<source-ip>	The source addresses to match against. You can specify a single host, a subnet, or all source addresses. The following are the valid formats for specifying the source:	
	`any`	Match any source IP address.
	`host` *<ip-addr>*	Match a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	Match any source IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> *<reverse-mask>*	Match any source IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<dest-ip>	The destination addresses to match against. You can specify a single host, a subnet, or all destination addresses. The following are the valid formats for specifying the destination:	
	`any`	Match any destination IP address.
	`host` *<ip-addr>*	Match a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	Match any destination IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.

Table 38-3: Parameters in **access-list (hardware IP numbered)** (cont.)

Parameter	Description	
	<ip-addr> *<reverse-mask>*	Match any destination IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
`vlan` *<1-4094>*	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Table 38-4: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]

Table 38-4: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode Global Configuration

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes This command creates an ACL for use with hardware classification. Once you have configured the ACL, use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map.

ACLs numbered in the range 3000-3699 match on packets that have the specified source and destination IP addresses.

Examples To create an access-list that will deny all IGMP packets (IP protocol 2) from the 192.168.0.0 network, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 deny proto 2 192.168.0.0/16
any
```

To destroy the access-list with an access-list identity of 3000 enter the following commands:

```
awplus# configure terminal
awplus(config)# no access-list 3000
```

Related commands access-group

match access-group

show running-config

show access-list (IPv4 Hardware ACLs)

access-list (numbered hardware ACL for MAC addresses)

Overview This command creates an access-list for use with hardware classification. The access-list will match on packets that have the specified source and destination MAC addresses. You can use the value **any** instead of source or destination address if an address does not matter.

Once you have configured the ACL, you can use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map.

The **no** variant of this command removes the specified MAC hardware filter access-list.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
access-list <4000-4699> <action> {<source-mac>|any}
{<dest-mac>|any} [vlan <1-4094>] [inner-vlan <1-4094>]

no access-list <4000-4699>
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Parameter	Description
<4000-4699>	Hardware MAC access-list.
<action>	The action that the switch will take on matching packets. See the table above for valid values.
<source-mac>	The source MAC address to match against, followed by the mask. Enter the address in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. Enter the mask in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. For a mask, each value is either 0 or F, where FF = Ignore, and 00 = Match.
`any`	Match against any source MAC address.
<dest-mac>	The destination MAC address to match against, followed by the mask. Enter the address in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. Enter the mask in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. For a mask, each value is either 0 or F, where FF = Ignore, and 00 = Match.
`any`	Match against any destination MAC address.
`vlan` *<1-4094>*	Match against the specified ID in the packet's VLAN tag.
`inner-vlan` *<1-4094>*	Match against the inner VLAN tag (VID). This parameter is used within double-tagged VLANs. It is sometimes referred to as the C-TAG (Customer VLAN TAG), where the vlan VID tag is referred to as the S-TAG (Service VLAN TAG).

Mode Global Configuration

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes This command creates an ACL for use with hardware classification. Once you have configured the ACL, use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map.

ACLs numbered in the range 4000-4699 match on packets that have the specified source and destination MAC addresses.

Examples To create an access-list that will permit packets with a source MAC address of 0000.00ab.1234 and any destination address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 4000 permit 0000.00ab.1234
0000.0000.0000 any
```

To create an access-list that will permit packets if their source MAC address starts with 0000.00ab, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 permit 0000.00ab.1234
0000.0000.FFFF any
```

To create an access-list that will send a copy of packets to the mirror port if their source MAC address starts with 0000.00ab, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 copy-to-mirror 0000.00ab.1234
0000.0000.FFFF any
```

You also need to configure the mirror port with the mirror interface command.

To destroy the access-list with an access-list identity of 4000 enter the commands:

```
awplus# configure terminal
awplus(config)# no access-list 4000
```

Related commands

access-group

match access-group

show running-config

show access-list (IPv4 Hardware ACLs)

Command changes

Version 5.4.7-2.1: **send-to-vlan-port** action parameter added to GS900MX, SBx8100, SBx908 GEN2, XS900MX series.

Version 5.4.6-2.1: **send-to-vlan-port** action parameter added

access-list (numbered hardware ACL for TCP or UDP)

Overview This command creates an access-list for use with hardware classification. The access-list will match on TCP or UDP packets that have the specified source and destination IP addresses and optionally, port values. You can use the value **any** instead of source or destination IP address if an address does not matter.

Once you have configured the ACL, you can use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map.

You can use the optional **vlan** parameter to match tagged (802.1q) packets.

The **no** variant of this command removes the specified IP hardware access-list.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
access-list <3000-3699> <action> {tcp|udp} <source-ip>
[<source-ports>] <dest-ip> [<dest-ports>] [vlan <1-4094>]

no access-list <3000-3699>
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Parameter	Description	
<3000-3699>	An ID number for this hardware IP access-list.	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
tcp	Match against TCP packets.	
udp	Match against UDP packets.	
<source-ip>	The source addresses to match against. You can specify a single host, a subnet, or all source addresses. The following are the valid formats for specifying the source:	
	any	Match any source IP address.
	host *<ip-addr>*	Match a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	Match any source IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> *<reverse-mask>*	Match any source IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<source-ports>	Match source TCP or UDP port numbers. Port numbers are specified as integers between 0 and 65535. You can specify one or more port numbers as follows:	
	eq <0-65535>	Match a single port number.
	lt <0-65535>	Match all port numbers that are less than the specified port number.
	gt <0-65535>	Match all port numbers that are greater than the specified port number.
	ne <0-65535>	Match all port numbers except the specified port number.
	range *<start-port>* *<end-port>*	Match a range of port numbers.
<dest-ip>	The destination addresses to match against. You can specify a single host, a subnet, or all destination addresses. The following are the valid formats for specifying the destination:	
	any	Match any destination IP address.
	host *<ip-addr>*	Match a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.

Parameter	Description	
	<ip-addr>/<prefix>	Match any destination IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> <reverse-mask>	Match any destination IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<dest-ports>	Match destination TCP or UDP port numbers. Port numbers are specified as integers between 0 and 65535. You can specify one or more port numbers as follows:	
	`eq <0-65535>`	Match a single port number.
	`lt <0-65535>`	Match all port numbers that are less than the specified port number.
	`gt <0-65535>`	Match all port numbers that are greater than the specified port number.
	`ne <0-65535>`	Match all port numbers except the specified port number.
	`range <start-port> <end-port>`	Match a range of port numbers.
`vlan <1-4094>`	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Mode Global Configuration

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes This command creates an ACL for use with hardware classification. Once you have configured the ACL, use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map.

ACLs numbered in the range 3000-3699 match on packets that have the specified source and destination IP addresses.

Examples To create an access-list that will permit TCP packets with a destination address of 192.168.1.1, a destination port of 80, and any source address and source port, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit tcp any 192.168.1.1/32 eq 80
```

To create an access-list that will copy TCP packets to the mirror port, if they have a destination address of 192.168.1.1, a destination port of 80, and any source address and source port, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 copy-to-mirror tcp any
192.168.1.1/32 eq 80
```

You also need to configure the mirror port with the mirror interface command.

Related commands

access-group

match access-group

show running-config

show access-list (IPv4 Hardware ACLs)

access-list hardware (named hardware ACL)

Overview This command creates a named hardware access-list and puts you into IPv4 Hardware ACL Configuration mode, where you can add filter entries to the ACL.

Once you have configured the ACL, you can use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map.

The **no** variant of this command removes the specified named hardware ACL.

Syntax

```
access-list hardware <name>
no access-list hardware <name>
```

Parameter	Description
<name>	Specify a name for the hardware ACL.

Mode Global Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage notes Use this command to name a hardware ACL and enter the IPv4 Hardware ACL Configuration mode. If the named hardware ACL does not exist, it will be created after entry. If the named hardware ACL already exists, then this command puts you into IPv4 Hardware ACL Configuration mode for that existing ACL.

Entering this command moves you to the IPv4 Hardware ACL Configuration mode (config-ip-hw-acl prompt), so you can enter ACL filters with sequence numbers. From this prompt, configure the filters for the ACL. See the ACL Feature Overview and Configuration Guide for complete examples of configured sequenced numbered ACLs.

NOTE: *Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples To create the hardware access-list named “ACL-1” and enter the IPv4 Hardware ACL Configuration mode to specify the ACL filter entry, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware ACL-1
awplus(config-ip-hw-acl)#
```

To remove the hardware access-list named “ACL-1”, use the commands:

```
awplus# configure terminal
awplus(config)# no access-list hardware ACL-1
```

Related commands

access-group

(named hardware ACL entry for ICMP)

(named hardware ACL entry for IP protocols)

(named hardware ACL entry for TCP or UDP)

(access-list standard named filter)

show access-list (IPv4 Hardware ACLs)

acl-group ip address

Overview Use this command to create a new named IPv4 ACL group that contains one or more IPv4 host or subnets.

This command creates a named IPv4 ACL group and enters the ACL Host Group config mode. IPv4 hosts or subnets can be added to or removed from this group. This host group can be used as a source or destination match for any hardware ACL to simplify large ACL configs with lots of IPv4 hosts.

Use the **no** variant of this command to delete an IPv4 ACL group.

Syntax

```
acl-group ip address <group>
no acl-group ip address <group>
```

Parameter	Description
<group>	The name of the IPv4 ACL group.

Default No ACL groups exist by default.

Mode Global Configuration

Example To create an IPv4 ACL group named IPV4 _GROUP1, use the commands:

```
awplus# configure terminal
awplus(config)# acl-group ip address IPV4_GROUP1
awplus(config-ip-host-group)#
```

To delete an IPv4 ACL group named IPV4 _GROUP1, use the commands:

```
awplus# configure terminal
awplus(config)# no acl-group ip address IPV4_GROUP1
```

Related commands ip (ip-host-group)

show acl-group ip address

Command changes Version 5.5.0-1.1: command added

acl-group ip port

Overview Use this command to create a new named port ACL group that contains one or more port rules for an ACL.

This command creates a named port ACL group and enters the ACL Port Group config mode. Port matching rules can be added to or removed from this group. This host group can be used to match on source or destination ports when used with an ACL.

Use the **no** variant of this command to delete a port ACL group.

Syntax

```
acl-group ip port <group>
no acl-group ip port <group>
```

Parameter	Description
<group>	The name of the port ACL group.

Default No ACL groups exist by default.

Mode Global Configuration

Example To create a port ACL group named PORT_GROUP1, use the commands:

```
awplus# configure terminal
awplus(config)# acl-group ip port PORT_GROUP1
awplus(config-ip-port-group)#
```

To delete a port ACL group named PORT_GROUP1, use the commands:

```
awplus# configure terminal
awplus(config)# no acl-group ip port PORT_GROUP1
```

Related commands (acl-group ip port range)

show acl-group ip port

Command changes Version 5.5.0-1.1: command added

(acl-group ip port range)

Overview Use this command to add one or more protocol port rules on a port ACL group. These port matching rules are used to simplify large ACL configs where many ACLs block or permit on the same service ports.

Use the **no** variant of this command to remove a rule match on protocol ports.

Syntax

```
eq <0-65535>
lt <0-65535>
gt <0-65535>
ne <0-65535>
range <0-65535> <0-65535>
no eq <0-65535>
no lt <0-65535>
no gt <0-65535>
no ne <0-65535>
no range <0-65535> <0-65535>
```

Parameter	Description
`eq`	The protocol port matches if equal to this number.
`lt`	The protocol port matches if less than this number.
`gt`	The protocol port matches if greater than this number.
`ne`	The protocol port matches if not equal to this number.
`range`	The protocol port matches if it is in this range.
<0-65535>	The port number.

Default The port ACL group will match on all ports by default.

Mode IP ACL Port Group Configuration

Example To add the rule match on protocol ports equal to 20 on a port ACL group, use the commands:

```
awplus# configure terminal
awplus(config)# acl-group ip port PORT_GROUP1
awplus(config-ip-port-group)# eq 20
```

To add the rule match on protocol ports between 20 and 50 on a port ACL group, use the commands:

```
awplus# configure terminal
awplus(config)# acl-group ip port PORT_GROUP1
awplus(config-ip-port-group)# range 20 50
```

To add the rule match on protocol ports greater than 20 except 30 on a port ACL group, use the commands:

```
awplus# configure terminal
awplus(config)# acl-group ip port PORT_GROUP1
awplus(config-ip-port-group)# gt 20
awplus(config-ip-port-group)# ne 30
```

To remove the rule match on protocol ports between 20 and 50 on a port ACL group, use the commands:

```
awplus# configure terminal
awplus(config)# acl-group ip port PORT_GROUP1
awplus(config-ip-port-group)# no range 20 50
```

Related commands

acl-group ip port

show acl-group ip port

Command changes

Version 5.5.0-1.1: command added

commit (IPv4)

Overview Use this command to commit the IPv4 ACL filter configuration entered at the console to the hardware immediately without exiting the IPv4 Hardware ACL Configuration mode.

This command forces the associated hardware and software IPv4 ACLs to synchronize.

Syntax

```
commit
```

Mode IPv4 Hardware ACL Configuration

Usage notes Normally, when an IPv4 hardware ACL is edited, the new configuration state of the IPv4 ACL is not written to hardware until you exit IPv4 Hardware ACL Configuration mode. By entering this command you can ensure that the current state of a hardware access-list that is being edited is written to hardware immediately.

Scripts typically do not include the exit command to exit configuration modes, potentially leading to IPv4 ACL filters in hardware not being correctly updated. Using this **commit** command in a configuration script after specifying an IPv4 hardware ACL filter ensures that it is updated in the hardware immediately.

Example To update the hardware with the IPv4 ACL filter configuration, use the command:

```
awplus# configure terminal
awplus(config)# access-list hardware my-hw-list
awplus(config-ip-hw-acl)# commit
```

Related commands access-list hardware (named hardware ACL)

ip (ip-host-group)

Overview Use this command to add an IPv4 host or subnet to an IPv4 ACL group. Adding IPv4 hosts and subnets to an ACL group allows you to simplify ACL config when the same IP addresses are required for many ACLs.

Use the **no** variant of this command to remove an IPv4 host or subnet from an IPv4 ACL group.

Syntax

```
ip {any|<match-ip>}
no ip {any|<match-ip>}
```

Parameter	Description	
`any`	Match any IP address.	
<match-ip>	The addresses to match against. You can specify a single host or a subnet. The following are the valid formats for specifying the addresses:	
	<ip-addr>	Match a single host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	Match any IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> <reverse-mask>	Match any IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.

Default No hosts or subnets are in an IPv4 ACL group by default.

Mode IP ACL Host Group Configuration

Example To add the subnet 192.168.1.0/24 to an IPv4 ACL group IPV4_GROUP1, use the commands:

```
awplus# configure terminal
awplus(config)# acl-group ip address IPV4_GROUP1
awplus(config-ip-host-group)# ip 192.168.1.0/24
```

To remove the subnet 192.168.1.0/24 from an IPv4 ACL group IPV4_GROUP1, use the commands:

```
awplus# configure terminal
awplus(config)# acl-group ip address IPV4_GROUP1
awplus(config-ip-host-group)# no ip 192.168.1.0/24
```

Related commands

acl-group ip address

show acl-group ip address

Command changes

Version 5.5.0-1.1: command added

(named hardware ACL entry for ICMP)

Overview

Use this command to add a new ICMP filter entry to the current hardware access-list. The filter will match on any ICMP packet that has the specified source and destination IP addresses and (optionally) ICMP type. You can specify the value **any** if source or destination address does not matter.

If you specify a sequence number, the switch inserts the new filter at the specified location. Otherwise, the switch adds the new filter to the end of the access-list.

The **no** variant of this command removes an ICMP filter entry from the current hardware access-list. You can specify the ICMP filter entry for removal by entering either its sequence number (e.g. **no 100**), or by entering its ICMP filter profile without specifying its sequence number (e.g. **no permit icmp 192.168.1.0/24 any icmp-type 11**).

You can find the sequence number by running the show access-list (IPv4 Hardware ACLs) command.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
[<sequence-number>] <action> icmp <source-ip> <dest-ip>
[icmp-type <number>] [vlan <1-4094>]

no <sequence-number>

no <action> icmp <source-ip> <dest-ip> [icmp-type <number>]
[vlan <1-4094>]
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.

Values for the <action> parameter	
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Parameter	Description	
<sequence-number>	The sequence number for the filter entry of the selected access control list, in the range 1-65535. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number. .	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
`icmp`	Match against ICMP packets	
<source-ip>	The source addresses to match against. You can specify a single host, a subnet, or all source addresses. The following are the valid formats for specifying the source:	
	`any`	Match any source IP address.
	`host <ip-addr>`	Match a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	Match any source IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> <reverse-mask>	Match any source IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<dest-ip>	The destination addresses to match against. You can specify a single host, a subnet, or all destination addresses. The following are the valid formats for specifying the destination:	
	`any`	Match any destination IP address.
	`host <ip-addr>`	Match a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.

Parameter	Description	
	`<ip-addr>/<prefix>`	Match any destination IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	`<ip-addr> <reverse-mask>`	Match any destination IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
`icmp-type <number>`	The type of ICMP message to match against, as defined in RFC792 and RFC950. Values include:	
	0	Echo replies.
	3	Destination unreachable messages.
	4	Source quench messages.
	5	Redirect (change route) messages.
	8	Echo requests.
	11	Time exceeded messages.
	12	Parameter problem messages.
	13	Timestamp requests.
	14	Timestamp replies.
	15	Information requests.
	16	Information replies.
	17	Address mask requests.
	18	Address mask replies.
`vlan <1-4094>`	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Mode IPv4 Hardware ACL Configuration (accessed by running the command access-list hardware (named hardware ACL))

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes To use this command, first run the command access-list hardware (named hardware ACL) and enter the desired access-list name. This changes the prompt to awplus(config-ip-hw-acl)#.

Then use this command (and the other "named hardware ACL: entry" commands) to add filter entries. You can add multiple filter entries to an ACL. You can insert a

new filter entry into the middle of an existing list by specifying the appropriate sequence number. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number.

Then use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map. Note that the ACL will only apply to incoming data packets.

Examples

To add an access-list filter entry with a sequence number of 100 to the access-list named "my-list" that will permit ICMP packets with a source address of 192.168.1.0/24, any destination address and an ICMP type of 5, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# 100 permit icmp 192.168.1.0/24 any
icmp-type 5
```

To remove an access-list filter entry with a sequence number of 100 from the access-list named "my-list", use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# no 100
```

Related commands

access-group

access-list hardware (named hardware ACL)

match access-group

show running-config

show access-list (IPv4 Hardware ACLs)

(named hardware ACL entry for IP packets)

Overview

Use this command to add an IP packet filter entry to the current hardware access-list. The filter will match on IP packets that have the specified IP and/or MAC addresses. You can use the value **any** instead of source or destination IP or MAC address if an address does not matter.

If you specify a sequence number, the switch inserts the new filter at the specified location. Otherwise, the switch adds the new filter to the end of the access-list.

The **no** variant of this command removes a filter entry from the current hardware access-list. You can specify the filter entry for removal by entering either its sequence number (e.g. **no 100**), or by entering its filter profile without specifying its sequence number (e.g. **no deny ip 192.168.0.0/16 any**).

You can find the sequence number by running the show access-list (IPv4 Hardware ACLs) command.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
[<sequence-number>] <action> ip <source-ip> <dest-ip>
[<source-mac> <dest-mac>] [vlan <1-4094>]

no <sequence-number>

no <action> ip <source-ip> <dest-ip> [<source-mac> <dest-mac>]
[vlan <1-4094>]
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Parameter	Description	
<sequence-number>	The sequence number for the filter entry of the selected access control list, in the range 1-65535. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number. .	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
ip	Match against IP packets	
<source-ip>	The source addresses to match against. You can specify a single host, a subnet, or all source addresses. The following are the valid formats for specifying the source:	
	any	Match any source IP address.
	dhcpsnooping	Match the source address learned from the DHCP Snooping binding database.
	host *<ip-addr>*	Match a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	Match any source IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> *<reverse-mask>*	Match any source IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<dest-ip>	The destination addresses to match against. You can specify a single host, a subnet, or all destination addresses. The following are the valid formats for specifying the destination:	
	any	Match any destination IP address.
	host *<ip-addr>*	Match a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	Match any destination IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.

Parameter	Description	
	<ip-addr> *<reverse-mask>*	Match any destination IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<source-mac>	The source MAC address to match against. You can specify a single MAC address, a range (through a mask), the address learned from DHCP snooping, or any:	
	`any`	Match against any source MAC address.
	<source-mac>	The source MAC address to match against, followed by the mask. Enter the address in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. Enter the mask in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. For a mask, each value is either 0 or F, where FF = Ignore, and 00 = Match.
	`dhcpsnooping`	Match the source address learned from the DHCP Snooping binding database.
<dest-mac>	The destination MAC address to match against. You can specify a single MAC address, a range (through a mask), or any:	
	`any`	Match against any destination MAC address.
	<dest-mac>	The destination MAC address to match against, followed by the mask. Enter the address in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. Enter the mask in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. For a mask, each value is either 0 or F, where FF = Ignore, and 00 = Match.
`vlan` *<1-4094>*	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Mode IPv4 Hardware ACL Configuration (accessed by running the command access-list hardware (named hardware ACL))

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes

To use this command, first run the command access-list hardware (named hardware ACL) and enter the desired access-list name. This changes the prompt to awplus(config-ip-hw-acl)#.

Then use this command (and the other "named hardware ACL: entry" commands) to add filter entries. You can add multiple filter entries to an ACL. You can insert a new filter entry into the middle of an existing list by specifying the appropriate sequence number. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number.

Then use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map. Note that the ACL will only apply to incoming data packets.

Examples

To add a filter entry to the access-list named "my-list" that will permit any IP packet with a source address of 192.168.1.1, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit ip 192.168.1.1/32 any
```

To add a filter entry to the access-list named "my-list" that will permit any IP packet with a source address of 192.168.1.1and a MAC source address of ffee.ddcc.bbaa, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit ip 192.168.1.1/32 any mac
ffee.ddcc.bbaa 0000.0000.0000 any
```

To add a filter entry to the access-list named "my-list" that will deny all IP packets on vlan 2, use the commands:

```
awplus# enable
awplus(config)# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# deny ip any any vlan 2
```

Related commands

access-group

access-list hardware (named hardware ACL)

match access-group

show running-config

show access-list (IPv4 Hardware ACLs)

(named hardware ACL entry for IP protocols)

Overview

Use this command to add an IP protocol type filter entry to the current hardware access-list. The filter will match on IP packets that have the specified IP protocol number, and the specified IP and/or MAC addresses. You can use the value **any** instead of source or destination IP or MAC address if an address does not matter.

If you specify a sequence number, the switch inserts the new filter at the specified location. Otherwise, the switch adds the new filter to the end of the access-list.

The **no** variant of this command removes a filter entry from the current hardware access-list. You can specify the filter entry for removal by entering either its sequence number (e.g. **no 100**), or by entering its filter profile without specifying its sequence number (e.g. **no deny proto 2 192.168.0.0/16 any**).

You can find the sequence number by running the show access-list (IPv4 Hardware ACLs) command.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
[<sequence-number>] <action> proto <1-255> <source-ip>
<dest-ip> [<source-mac> <dest-mac>] [vlan <1-4094>]

no <sequence-number>

no <action> proto <1-255> <source-ip> <dest-ip> [<source-mac>
<dest-mac>] [vlan <1-4094>]
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Table 38-5: Parameters in IP protocol ACL entries

Parameter	Description	
<sequence-number>	The sequence number for the filter entry of the selected access control list, in the range 1-65535. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number. .	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
`proto` *<1-255>*	The IP protocol number to match against, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.	
<source-ip>	The source addresses to match against. You can specify a single host, a subnet, or all source addresses. The following are the valid formats for specifying the source:	
	`any`	Match any source IP address.
	`dhcpsnooping`	Match the source address learned from the DHCP Snooping binding database.
	`host` *<ip-addr>*	Match a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	Match any source IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> *<reverse-mask>*	Match any source IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<dest-ip>	The destination addresses to match against. You can specify a single host, a subnet, or all destination addresses. The following are the valid formats for specifying the destination:	
	`any`	Match any destination IP address.
	`host` *<ip-addr>*	Match a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	Match any destination IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.

Table 38-5: Parameters in IP protocol ACL entries (cont.)

Parameter	Description	
	<ip-addr> *<reverse-mask>*	Match any destination IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<source-mac>	The source MAC address to match against. You can specify a single MAC address, a range (through a mask), the address learned from DHCP snooping, or any:	
	`any`	Match against any source MAC address.
	<source-mac>	The source MAC address to match against, followed by the mask. Enter the address in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. Enter the mask in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. For a mask, each value is either 0 or F, where FF = Ignore, and 00 = Match.
	`dhcpsnooping`	Match the source address learned from the DHCP Snooping binding database.
<dest-mac>	The destination MAC address to match against. You can specify a single MAC address, a range (through a mask), or any:	
	`any`	Match against any destination MAC address.
	<dest-mac>	The destination MAC address to match against, followed by the mask. Enter the address in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. Enter the mask in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. For a mask, each value is either 0 or F, where FF = Ignore, and 00 = Match.
`vlan` *<1-4094>*	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Table 38-6: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828

Table 38-6: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode IPv4 Hardware ACL Configuration (accessed by running the command access-list hardware (named hardware ACL))

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes To use this command, run the command access-list hardware (named hardware ACL) and enter the desired access-list name. This changes the prompt to awplus(config-ip-hw-acl)#.

Then use this command (and the other "named hardware ACL: entry" commands) to add filter entries. You can add multiple filter entries to an ACL. You can insert a new filter entry into the middle of an existing list by specifying the appropriate sequence number. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number.

Then use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map. Note that the ACL will only apply to incoming data packets.

Examples To add a filter entry to the access-list named "my-list" that will deny all IGMP packets (protocol 2) from the 192.168.0.0 subnet, and give it a sequence number of 50, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# 50 deny proto 2 192.168.0.0/16 any
```

Related commands

access-group

access-list hardware (named hardware ACL)

match access-group

show running-config

show access-list (IPv4 Hardware ACLs)

(named hardware ACL entry for MAC addresses)

Overview Use this command to add a MAC address filter entry to the current hardware access-list. The access-list will match on packets that have the specified source and destination MAC addresses. You can use the value **any** instead of source or destination MAC address if an address does not matter.

If you specify a sequence number, the switch inserts the new filter at the specified location. Otherwise, the switch adds the new filter to the end of the access-list.

The **no** variant of this command removes a filter entry from the current hardware access-list. You can specify the filter entry for removal by entering either its sequence number (e.g. **no 100**), or by entering its filter profile without specifying its sequence number (e.g. **no permit mac aaaa.bbbb.cccc 0000.0000.0000 any**).

You can find the sequence number by running the show access-list (IPv4 Hardware ACLs) command.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
[<sequence-number>] <action> mac {<source-mac>|any}
{<dest-mac>|any} [vlan <1-4094>] [inner-vlan <1-4094>]

no <sequence-number>

no <action> mac {<source-mac>|any} {<dest-mac>|any} [vlan
<1-4094>] [inner-vlan <1-4094>]
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.

Values for the <action> parameter	
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Parameter	Description
<4000-4699>	Hardware MAC access-list.
<action>	The action that the switch will take on matching packets. See the table above for valid values.
`mac`	Match against MAC address
<source-mac>	The source MAC address to match against, followed by the mask. Enter the address in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. Enter the mask in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. For a mask, each value is either 0 or F, where FF = Ignore, and 00 = Match.
`any`	Match against any source MAC address.
<dest-mac>	The destination MAC address to match against, followed by the mask. Enter the address in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. Enter the mask in the format <HHHH.HHHH.HHHH>, where each *H* is a hexadecimal number. For a mask, each value is either 0 or F, where FF = Ignore, and 00 = Match.
`any`	Match against any destination MAC address.
`vlan` *<1-4094>*	Match against the specified ID in the packet's VLAN tag.
`inner-vlan` *<1-4094>*	Match against the inner VLAN tag (VID). This parameter is used within double-tagged VLANs. It is sometimes referred to as the C-TAG (Customer VLAN TAG), and the vlan VID tag is referred to as the S-TAG (Service VLAN TAG).

Mode IPv4 Hardware ACL Configuration (accessed by running the command access-list hardware (named hardware ACL))

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes To use this command, first run the command access-list hardware (named hardware ACL) and enter the desired access-list name. This changes the prompt to awplus(config-ip-hw-acl)#.

Then use this command (and the other "named hardware ACL: entry" commands) to add filter entries. You can add multiple filter entries to an ACL. You can insert a new filter entry into the middle of an existing list by specifying the appropriate

sequence number. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number.

Then use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map. Note that the ACL will only apply to incoming data packets.

Examples

To add a filter entry to the access-list named "my-list" that will permit packets with a source MAC address of 0000.00ab.1234 and any destination MAC address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit mac 0000.00ab.1234
0000.0000.0000 any
```

To remove a filter entry that permit packets with a source MAC address of 0000.00ab.1234 and any destination MAC address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# no permit mac 0000.00ab.1234
0000.0000.0000 any
```

Related commands

access-group

access-list hardware (named hardware ACL)

match access-group

show running-config

show access-list (IPv4 Hardware ACLs)

Command changes

Version 5.4.7-2.1: **send-to-vlan-port** action parameter added to GS900MX, SBx8100, SBx908 GEN2, XS900MX series.

Version 5.4.6-2.1: **send-to-vlan-port** action parameter added

(named hardware ACL entry for TCP or UDP)

Overview

Use this command to add a TCP or UDP filter entry to the current hardware access-list. The access-list will match on TCP or UDP packets that have the specified source and destination IP addresses and optionally, port values. You can use the value **any** instead of source or destination IP address if an address does not matter.

If you specify a sequence number, the switch inserts the new filter at the specified location. Otherwise, the switch adds the new filter to the end of the access-list.

The **no** variant of this command removes a filter entry from the current hardware access-list. You can specify the filter entry for removal by entering either its sequence number (e.g. **no 100**), or by entering its filter profile without specifying its sequence number (e.g. **no permit udp 192.168.0.0/16 any**).

You can find the sequence number by running the show access-list (IPv4 Hardware ACLs) command.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
[<sequence-number>] <action> {tcp|udp} <source-ip>
[<source-ports>] <dest-ip> [<dest-ports>] [vlan <1-4094>]

no <sequence-number>

no <action> {tcp|udp} <source-ip> [<source-ports>] <dest-ip>
[<dest-ports>] [vlan <1-4094>]
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Parameter	Description	
<sequence-number>	The sequence number for the filter entry of the selected access control list, in the range 1-65535. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number. .	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
`tcp`	Match against TCP packets.	
`udp`	Match against UDP packets.	
<source-ip>	The source addresses to match against. You can specify a single host, a subnet, or all source addresses. The following are the valid formats for specifying the source:	
	`any`	Match any source IP address.
	`host <ip-addr>`	Match a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	Match any source IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> <reverse-mask>	Match any source IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<source-ports>	Match source TCP or UDP port numbers. Port numbers are specified as integers between 0 and 65535. You can specify one or more port numbers as follows:	
	`eq <0-65535>`	Match a single port number.
	`lt <0-65535>`	Match all port numbers that are less than the specified port number.
	`gt <0-65535>`	Match all port numbers that are greater than the specified port number.
	`ne <0-65535>`	Match all port numbers except the specified port number.
	`range <start-port> <end-port>`	Match a range of port numbers.
<dest-ip>	The destination addresses to match against. You can specify a single host, a subnet, or all destination addresses. The following are the valid formats for specifying the destination:	

Parameter	Description	
	`any`	Match any destination IP address.
	`host <ip-addr>`	Match a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	`<ip-addr>/<prefix>`	Match any destination IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	`<ip-addr> <reverse-mask>`	Match any destination IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
`<dest-ports>`	Match destination TCP or UDP port numbers. Port numbers are specified as integers between 0 and 65535. You can specify one or more port numbers as follows:	
	`eq <0-65535>`	Match a single port number.
	`lt <0-65535>`	Match all port numbers that are less than the specified port number.
	`gt <0-65535>`	Match all port numbers that are greater than the specified port number.
	`ne <0-65535>`	Match all port numbers except the specified port number.
	`range <start-port> <end-port>`	Match a range of port numbers.
`vlan <1-4094>`	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Mode IPv4 Hardware ACL Configuration (accessed by running the command access-list hardware (named hardware ACL))

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes To use this command, first run the command access-list hardware (named hardware ACL) and enter the desired access-list name. This changes the prompt to awplus(config-ip-hw-acl)#.

Then use this command (and the other "named hardware ACL: entry" commands) to add filter entries. You can add multiple filter entries to an ACL. You can insert a new filter entry into the middle of an existing list by specifying the appropriate sequence number. If you do not specify a sequence number, the switch puts the

entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number.

Then use the access-group or the match access-group command to apply this ACL to a port, VLAN or QoS class-map. Note that the ACL will only apply to incoming data packets.

Example To add a filter entry to access-list named "my-list" that will permit TCP packets with a destination address of 192.168.1.1, a destination port of 80, from any source, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit tcp any 192.168.1.1/32 eq 80
```

Related commands

access-group

access-list hardware (named hardware ACL)

match access-group

show running-config

show access-list (IPv4 Hardware ACLs)

show access-group

Overview Use this command to show the access-lists attached globally. If an access-list is specified, only that access-list will be displayed.

Syntax

```
show access-group
[{<3000-3699>|<4000-4699>|<access-list-name>}]
```

Parameter	Description
<3000-3699>	Specify a Hardware IP access-list.
<4000-4699>	Specify a Hardware MAC access-list.
<access-list-name>	Specify a Hardware IPv4 access-list name.

Mode User Exec and Privileged Exec

Example To show all access-lists attached globally:

```
awplus# show access-group
```

Output Figure 38-1: Example output from the show access-group command

```
Global access control list
access-group 3000
access-group 4000
```

Related commands

access-group

show interface access-group

show access-list (IPv4 Hardware ACLs)

Overview Use this command to display the specified access-list, or all access-lists if none have been specified. Note that only defined access-lists are displayed. An error message is displayed for an undefined access-list.

Syntax

```
show access-list
[<1-99>|<100-199>|<1300-1999>|<2000-2699>|<3000-3699>|
<4000-4499>|<access-list-name>]
```

Parameter	Description
<1-99>	IP standard access-list.
<100-199>	IP extended access-list.
<1300-1999>	IP standard access-list (standard - expanded range).
<2000-2699>	IP extended access-list (extended - expanded range).
<3000-3699>	Hardware IP access-list.
<4000-4499>	Hardware MAC access-list.
<access-list-name>	IP named access-list.

Mode User Exec and Privileged Exec

Examples To show all access-lists configured on the switch:

```
awplus# show access-list
```

```
Standard IP access list 1
    deny 172.16.2.0, wildcard bits 0.0.0.255
Standard IP access list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
Hardware IP access list 3001
    permit ip 192.168.20.0 255.255.255.0 any
Hardware IP access list 3020
    permit tcp any 192.0.2.0/24
```

To show the access-list with an ID of 20:

```
awplus# show access-list 20
```

```
Standard IP access-list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
```

The following error message is displayed if you try to show an undefined access-list.

```
awplus# show access-list 2
```

```
% Can't find access-list 2
```

Related commands

access-list extended (named)

access-list (numbered hardware ACL for MAC addresses)

access-list hardware (named hardware ACL)

show acl-group ip address

Overview Use this command to show the hosts and subnets in a named IPv4 ACL group.

Syntax

```
show acl-group ip address <group>
```

Parameter	Description
<group>	The name of the IPv4 ACL group.

Mode Privileged Exec

Example To show all hosts and subnets in an IPv4 ACL group IPV4_GROUP1, use the command:

```
awplus# show acl-group ip address IPV4_GROUP1
```

Output Figure 38-2: Example output from **show acl-group ip address IPV4_GROUP1**

```
awplus#show acl-group ip address IPV4_GROUP1
Host Group: IPV4_GROUP1

 192.168.1.2/32
 192.168.2.5/32
 10.0.0.0/8
```

Related commands acl-group ip address

ip (ip-host-group)

Command changes Version 5.5.0-1.1: command added

show acl-group ip port

Overview Use this command to show the port rules in a named port ACL group.

Syntax

```
show acl-group ip port <group>
```

Parameter	Description
<group>	The name of the port ACL group.

Mode Privileged Exec

Example To show all port rules in a port ACL group PORT_GROUP1, use the command:

```
awplus# show acl-group ip port PORT_GROUP1
```

Output Figure 38-3: Example output from **show acl-group ip port PORT_GROUP1**

```
awplus#show acl-group ip port PORT_GROUP1
Port Group: PORT_GROUP1

 eq 11
 gt 20
 lt 503
 ne 500
```

Related commands (acl-group ip port range)

acl-group ip port

Command changes Version 5.5.0-1.1: command added

show interface access-group

Overview Use this command to display the access groups attached to a port. If an access group is specified, then the output only includes the ports that the specified access group is attached to. If no access group is specified then this command displays all access groups that are attached to the ports that are specified with <port-list>.

Note that **access group** is the term given for an access-list when it is applied to an interface.

Syntax

```
show interface <port-list> access-group
[<3000-3699>|<4000-4699>]
```

Parameter	Description
<port-list>	Specify the ports to display information. A port-list can be either: • a switch port (e.g. port1.0.6) a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2) • a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.6 or port1.0.1-port1.0.6 or po1-po2 • a comma-separated list of ports and port ranges, e.g. port1.0.1,port1.0.3-1.0.6. Do not mix switch ports, static channel groups, and LACP channel groups in the same list.
`access group`	Select the access group whose details you want to show.
<3000-3699>	Specifies the Hardware IP access-list.
<4000-4699>	Specifies the Hardware MAC access-list.

Mode User Exec and Privileged Exec

Example To show all access-lists attached to port1.0.1, use the command:

```
awplus# show interface port1.0.1 access-group
```

Output Figure 38-4: Example output from the **show interface access-group** command

```
Interface port1.0.1
  access-group 3000
  access-group 3002
  access-group 3001
```

Related commands access-group

39 IPv4 Software Access Control List (ACL) Commands

Introduction

Overview This chapter provides an alphabetical reference for the IPv4 Software Access Control List (ACL) commands, and contains detailed command information and command examples about IPv4 software ACLs as applied to Routing and Multicasting, which are not applied to interfaces.

For information about ACLs, see the ACL Feature Overview and Configuration Guide.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see the following references:

- the Link Aggregation Feature Overview_and_Configuration_Guide.
- Link Aggregation Commands

NOTE: *Text in parenthesis in command names indicates usage not keyword entry. For example,* ***access-list hardware (named)*** *indicates named IPv4 hardware ACLs entered as* `access-list hardware <name>` *where <name> is a placeholder not a keyword.*

Parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as ***(access-list standard numbered filter)*** *represents command entry in the format shown in the syntax:*

```
[<sequence-number>] {deny|permit} {<source-address>|host
<host-address>|any}
```

NOTE: *Software ACLs will* ***deny*** *access unless* ***explicitly permitted*** *by an ACL action.*

Sub-modes Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 39-1: IPv4 Software Access List Commands and Prompts

Command Name	Command Mode	Prompt
clear ip prefix-list	Privileged Exec	awplus#
show ip access-list	Privileged Exec	awplus#
show ip prefix-list	Privileged Exec	awplus#
access-group	Global Configuration	awplus(config)#
access-list (extended named)	Global Configuration	awplus(config)#
access-list (extended numbered)	Global Configuration	awplus(config)#
access-list (standard named)	Global Configuration	awplus(config)#
access-list (standard numbered)	Global Configuration	awplus(config)#
ip prefix-list	Global Configuration	awplus(config)#
maximum-access-list	Global Configuration	awplus(config)#
dos	Interface Configuration	awplus(config-if)#
(access-list extended ICMP filter)	IPv4 Extended ACL Configuration	awplus(config-ip-ext-acl)#
(access-list extended IP filter)	IPv4 Extended ACL Configuration	awplus(config-ip-ext-acl)#
(access-list extended IP protocol filter)	IPv4 Extended ACL Configuration	awplus(config-ip-ext-acl)#
(access-list extended TCP UDP filter)	IPv4 Extended ACL Configuration	awplus(config-ip-ext-acl)#
(access-list standard named filter)	IPv4 Standard ACL Configuration	awplus(config-ip-std-acl)#
(access-list standard numbered filter)	IPv4 Standard ACL Configuration	awplus(config-ip-std-acl)#

Command List

- "access-list extended (named)" on page 1968
- "access-list (extended numbered)" on page 1976
- "(access-list extended ICMP filter)" on page 1979
- "(access-list extended IP filter)" on page 1981
- "(access-list extended IP protocol filter)" on page 1984
- "(access-list extended TCP UDP filter)" on page 1988
- "access-list standard (named)" on page 1991
- "access-list (standard numbered)" on page 1993
- "(access-list standard named filter)" on page 1995
- "(access-list standard numbered filter)" on page 1997

- "clear ip prefix-list" on page 1999
- "dos" on page 2000
- "ip prefix-list" on page 2003
- "maximum-access-list (deleted)" on page 2005
- "show access-list (IPv4 Software ACLs)" on page 2006
- "show dos interface" on page 2008
- "show ip access-list" on page 2011
- "show ip prefix-list" on page 2012
- "vty access-class (numbered)" on page 2013

access-list extended (named)

Overview

This command configures an extended named access-list that permits or denies packets from specific source and destination IP addresses. You can:

- use this command to enter a new or existing ACL name and enter the IPv4 Extended ACL Configuration mode. Once in that mode, you can create an ACL filter entry. This approach lets you give the entry a sequence number.
- or, use this command to create an ACL and an ACL filter entry at the same time. With this approach, you cannot give the entry a sequence number, so the entry will go after any existing entries.

The **no** variant of this command removes a specified extended named access-list.

Syntax [to enter the sub-mode]

```
access-list extended <list-name>
no access-list extended <list-name>
```

Parameter	Description
<list-name>	A user-defined name for the access-list

Syntax [icmp]

```
access-list extended <list-name> {deny|permit} icmp <source>
<destination> [icmp-type <type-number>] [log]
no access-list extended <list-name> {deny|permit} icmp <source>
<destination> [icmp-type <type-number>] [log]
```

Table 39-2: Parameters in the access-list extended (named) command - icmp

Parameter	Description
<list-name>	A user-defined name for the access-list.
deny	The access-list rejects packets that match the type, source, and destination filtering specified with this command.
permit	The access-list permits packets that match the type, source, and destination filtering specified with this command.
icmp	The access-list matches only ICMP packets.
icmp-type	Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets.

Table 39-2: Parameters in the access-list extended (named) command - icmp

Parameter	Description	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.

Table 39-2: Parameters in the access-list extended (named) command - icmp

Parameter	Description	
<type-number>	The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type:	
	0	Echo replies.
	3	Destination unreachable messages.
	4	Source quench messages.
	5	Redirect (change route) messages.
	8	Echo requests.
	11	Time exceeded messages.
	12	Parameter problem messages.
	13	Timestamp requests.
	14	Timestamp replies.
	15	Information requests.
	16	Information replies.
	17	Address mask requests.
	18	Address mask replies.
`log`	Logs the results.	

Syntax [tcp|udp]

```
access-list extended <list-name> {deny|permit} {tcp|udp}
<source> [eq <sourceport>|lt <sourceport>|gt <sourceport>|ne
<sourceport>] <destination> [eq <destport>|lt <destport>|gt
<destport>|ne <destport>] [log]
```

```
no access-list extended <list-name> {deny|permit} {tcp|udp}
<source> [eq <sourceport>|lt <sourceport>|gt <sourceport>|ne
<sourceport>] <destination> [eq <destport> |lt <destport>|gt
<destport>|ne <destport>][log]
```

Table 39-3: Parameters in the access-list extended (named) command - tcp|udp

Parameter	Description
<list-name>	A user-defined name for the access-list.
`deny`	The access-list rejects packets that match the type, source, and destination filtering specified with this command.
`permit`	The access-list permits packets that match the type, source, and destination filtering specified with this command.
`tcp`	The access-list matches only TCP packets.
`udp`	The access-list matches only UDP packets.

Table 39-3: Parameters in the access-list extended (named) command - tcp|udp

Parameter	Description	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> <reverse-mask>	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> <reverse-mask>	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<sourceport>	The source port number, specified as an integer between 0 and 65535.	
<destport>	The destination port number, specified as an integer between 0 and 65535.	
`eq`	Matches port numbers equal to the port number specified immediately after this parameter.	
`lt`	Matches port numbers less than the port number specified immediately after this parameter.	
`gt`	Matches port numbers greater than the port number specified immediately after this parameter.	

Table 39-3: Parameters in the access-list extended (named) command - tcp|udp

Parameter	Description
ne	Matches port numbers not equal to the port number specified immediately after this parameter.
log	Log the results.

Syntax [proto|any| ip]

```
access-list extended <list-name> {deny|permit} {proto
<ip-protocol>|any|ip} {<source>} {<destination>} [log]
```

```
no access-list extended <list-name>{deny|permit} {proto
<ip-protocol>|any|ip}{<source>}{<destination>}[log]
```

Table 39-4: Parameters in the access-list extended (named) command - proto|ip|any

Parameter	Description	
<list-name>	A user-defined name for the access-list.	
deny	The access-list rejects packets that match the type, source, and destination filtering specified with this command.	
permit	The access-list permits packets that match the type, source, and destination filtering specified with this command.	
proto	Matches only a specified type of IP Protocol.	
any	The access-list matches any type of IP packet.	
ip	The access-list matches only IP packets.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	any	Matches any source IP address.
	host *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.

Table 39-4: Parameters in the access-list extended (named) command - proto|ip|any (cont.)

Parameter	Description	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/ *<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
`log`	Logs the results.	
<ip-protocol>	The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.	

Table 39-5: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]

Table 39-5: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use this command when configuring access-lists for filtering IP software packets.

You can either create access-lists from within this command, or you can enter **access-list extended** followed by only the name. Entering only the name moves you to the IPv4 Extended ACL Configuration mode for the selected access-list.

From there you can configure your access-lists by using the commands (access-list extended ICMP filter), (access-list extended IP filter), and (access-list extended IP protocol filter).

Note that packets must match both the source and the destination details.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples

You can enter the extended named ACL in the Global Configuration mode together with the ACL filter entry on the same line, as shown below:

```
awplus# configure terminal
awplus(config)# access-list extended TK deny tcp 2.2.2.3/24 eq 14 3.3.3.4/24 eq 12 log
```

Alternatively, you can enter the extended named ACL in Global Configuration mode before specifying the ACL filter entry in the IPv4 Extended ACL Configuration mode, as shown below:

```
awplus# configure terminal
awplus(config)# access-list extended TK
awplus(config-ip-ext-acl)# deny tcp 2.2.2.3/24 eq 14 3.3.3.4/24 eq 12 log
```

Related commands

(access-list extended ICMP filter)

(access-list extended IP filter)

(access-list extended TCP UDP filter)

show running-config

show ip access-list

access-list (extended numbered)

Overview

This command configures an extended numbered access-list that permits or denies packets from specific source and destination IP addresses. You can:

- use this command to enter a new or existing ACL number and enter the IPv4 Extended ACL Configuration mode. Once in that mode, you can create an ACL filter entry. This approach lets you give the entry a sequence number.
- or, use this command to create an ACL and an ACL filter entry at the same time. With this approach, you cannot give the entry a sequence number, so the entry will go after any existing entries.

The **no** variant of this command removes a specified extended named access-list.

Syntax [to enter the sub-mode]

```
access-list {<100-199>|<2000-2699>}
no access-list {<100-199>|<2000-2699>}
```

Syntax [to create an ACL entry]

```
access-list {<100-199>|<2000-2699>} {deny|permit} ip <source> <destination>
no access-list {<100-199>|<2000-2699>} {deny|permit} ip <source> <destination>
```

Parameter	Description	
<100-199>	IP extended access-list.	
<2000-2699>	IP extended access-list (expanded range).	
`deny`	Access-list rejects packets that match the source and destination filtering specified with this command.	
`permit`	Access-list permits packets that match the source and destination filtering specified with this command.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host` *<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr> *<reverse-mask>*	An IPv4 address, followed by a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`. This matches any source IP address within the specified subnet.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	

Parameter	Description	
	`any`	Matches any destination IP address.
	`host <ip-addr>`	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	`<ip-addr> <reverse-mask>`	An IPv4 address, followed by a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`. This matches any destination IP address within the specified subnet.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes Use this command when configuring access-list for filtering IP software packets.

You can either create access-lists from within this command, or you can enter **access-list** followed by only the number. Entering only the number moves you to the IPv4 Extended ACL Configuration mode for the selected access-list. From there you can configure your access-lists by using the commands (access-list extended ICMP filter), (access-list extended IP filter), and (access-list extended IP protocol filter).

Note that packets must match both the source and the destination details.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples You can enter the extended ACL in the Global Configuration mode together with the ACL filter entry on the same line, as shown below:

```
awplus# configure terminal
awplus(config)# access-list 101 deny ip 172.16.10.0 0.0.0.255 any
```

Alternatively, you can enter the extended ACL in Global Configuration mode before specifying the ACL filter entry in the IPv4 Extended ACL Configuration mode, as shown below:

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)# deny ip 172.16.10.0 0.0.0.255 any
```

Related commands

(access-list extended ICMP filter)

(access-list extended IP filter)

(access-list extended TCP UDP filter)

show running-config

show ip access-list

(access-list extended ICMP filter)

Overview Use this ACL filter to add a new ICMP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an ICMP filter entry from the current extended access-list. You can specify the ICMP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its ICMP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax [icmp]

```
[<sequence-number>] {deny|permit} icmp <source> <destination>
[icmp-type <icmp-value>] [log]
```

```
no {deny|permit} icmp <source> <destination>[icmp-type
<icmp-value>] [log]
```

```
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets that match the source and destination filtering specified with this command.	
permit	Access-list permits packets that match the source and destination filtering specified with this command.	
icmp	ICMP packet type.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	any	Matches any source IP address.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	any	Matches any destination IP address.

Parameter	Description
`icmp-type`	The ICMP type.
`<icmp-value>`	The value of the ICMP type.
`log`	Log the results.

Mode IPv4 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list (extended numbered) command or the access-list extended (named) command, with the required access control list number, or name - but with no further parameters selected.*

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To add a new entry in access-list called `my-list` that will reject ICMP packets from `10.0.0.1` to `192.168.1.1`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny icmp 10.0.0.1/32 192.168.1.1/32
```

Use the following commands to add a new filter at sequence number `5` position of the access-list called `my-list`. The filter will accept the ICMP type `8` packets from `10.1.1.0/24` network, to `192.168.1.0` network:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit icmp 10.1.1.0/24
192.168.1.0/24 icmp-type 8
```

Related commands access-group

show running-config

show ip access-list

(access-list extended IP filter)

Overview Use this ACL filter to add a new IP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP filter entry from the current extended access-list. You can specify the IP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax [ip]

```
[<sequence-number>] {deny|permit} ip <source> <destination>
no {deny|permit} ip <source> <destination>
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
`deny`	Access-list rejects packets that match the source and destination filtering specified with this command.	
`permit`	Access-list permits packets that match the source and destination filtering specified with this command.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host <ip-addr>`	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr> *<reverse-mask>*	Alternatively, enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, enter `192.168.1.1 0.0.0.255`.

Parameter	Description	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr> *<reverse-mask>*	Alternatively, enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, enter `192.168.1.1 0.0.0.255`.

Mode Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list (extended numbered) command or the access-list extended (named) command, with the required access control list number, or name - but with no further parameters selected.*

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example 1 [list-number] First use the following commands to enter the IPv4 Extended ACL Configuration mode and define a numbered extended access-list `101`:

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)#
```

Then use the following commands to add a new entry to the numbered extended access- list `101` that will reject packets from `10.0.0.1` to `192.168.1.1`:

```
awplus(config-ip-ext-acl)# deny ip host 10.0.0.1 host
192.168.1.1
awplus(config-ip-ext-acl)# 20 permit ip any any
```

Example 2 [list-name] First use the following commands to enter the IPv4 Extended ACL Configuration mode and define a named access-list called `my-acl`:

```
awplus# configure terminal
awplus(config)# access-list extended my-acl
awplus(config-ip-ext-acl)#
```

Then use the following commands to add a new entry to the named access-list `my-acl` that will reject packets from `10.0.0.1` to `192.168.1.1`:

```
awplus(config-ip-ext-acl)# deny ip host 10.0.0.1 host
192.168.1.1
awplus(config-ip-ext-acl)# 20 permit ip any any
```

Example 3 [list-number]

Use the following commands to remove the access-list filter entry with sequence number `20` from extended numbered access-list `101`.

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)# no 20
```

Example 4 [list-name]

Use the following commands to remove the access-list filter entry with sequence number `20` from extended named access-list `my-acl`:

```
awplus# configure terminal
awplus(config)# access-list extended my-acl
awplus(config-ip-ext-acl)# no 20
```

Related commands

access-list extended (named)

access-list (extended numbered)

show running-config

show ip access-list

(access-list extended IP protocol filter)

Overview Use this ACL filter to add a new IP protocol type filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP protocol filter entry from the current extended access-list. You can specify the IP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax [proto]

```
[<sequence-number>] {deny|permit} proto <ip-protocol> <source> <destination> [log]
no {deny|permit} proto <ip-protocol> <source> <destination> [log]
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets that match the source and destination filtering specified with this command.	
permit	Access-list permits packets that match the source and destination filtering specified with this command.	
proto *<ip-protocol>*	<1-255> Specify IP protocol number, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	any	Matches any source IP address.

Parameter	Description	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	`any`	Matches any destination IP address.
`log`	Log the results.	

Table 39-6: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]

Table 39-6: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode IPv4 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list (extended numbered) command or the access-list extended (named) command, with the required access control list number, or name - but with no further parameters selected.*

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example 1 [creating a list] Use the following commands to add a new access-list filter entry to the access-list named `my-list` that will reject IP packets from source address `10.10.1.1/32` to destination address `192.68.1.1/32`:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny ip 10.10.1.1/32 192.168.1.1/32
```

Example 2 [adding to a list]

Use the following commands to add a new access-list filter entry at sequence position `5` in the access-list named `my-list` that will accept packets from source address `10.10.1.1/24` to destination address `192.68.1.1/24`:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit ip 10.10.1.1/24
192.168.1.1/ 24
```

Related commands

access-list extended (named)

access-list (extended numbered)

show running-config

show ip access-list

(access-list extended TCP UDP filter)

Overview Use this ACL filter to add a new TCP or UDP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a TCP or UDP filter entry from the current extended access-list. You can specify the TCP or UDP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its TCP or UDP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax [tcp|udp]

```
[<sequence-number>] {deny|permit} {tcp|udp} <source> {eq
<sourceport> |lt <sourceport>|gt <sourceport>|ne <sourceport>}
<destination> [eq <destport>|lt <destport>|gt <destport>|ne
<destport>] [log]
```

```
no [<sequence-number>]{deny|permit} {tcp|udp} <source> {eq
<sourceport> |lt <sourceport>|gt <sourceport>|ne <sourceport>}
<destination> [eq <destport>|lt <destport>|gt <destport>|ne
<destport>] [log]
```

```
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets that match the source and destination filtering specified with this command.	
permit	Access-list permits packets that match the source and destination filtering specified with this command.	
tcp	The access-list matches only TCP packets.	
udp	The access-list matches only UDP packets.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	any	Matches any source IP address.
<sourceport>	The source port number, specified as an integer between 0 and 65535.	

Parameter	Description	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	`any`	Matches any destination IP address.
<destport>	The destination port number, specified as an integer between 0 and 65535.	
`eq`	Matches port numbers equal to the port number specified immediately after this parameter.	
`lt`	Matches port numbers less than the port number specified immediately after this parameter.	
`gt`	Matches port numbers greater than the port number specified immediately after this parameter.	
`ne`	Matches port numbers not equal to the port number specified immediately after this parameter.	
`log`	Log the results.	

Mode IPv4 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list (extended numbered) command or the access-list extended (named) command, with the required access control list number, or name - but with no further parameters selected.*

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example 1 [creating a list] To add a new entry to the access-list named `my-list` that will reject TCP packets from `10.0.0.1`on TCP port `10` to `192.168.1.1` on TCP port `20`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny tcp 10.0.0.1/32 eq 10
192.168.1.1/32 eq 20
```

Example 2 [adding to a list]

To insert a new entry with sequence number `5` of the access-list named `my-list` that will accept UDP packets from `10.1.1.0/24` network to `192.168.1.0/24` network on UDP port `80`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit udp 10.1.1.0/24
192.168.1.0/24 eq 80
```

Related commands

access-list extended (named)

access-list (extended numbered)

show running-config

show ip access-list

access-list standard (named)

Overview This command configures a standard named access-list that permits or denies packets from a specific source IP address. You can:

- use this command to enter a new or existing ACL name and enter the IPv4 Standard ACL Configuration mode. Once in that mode, you can create an ACL filter entry using the command (access-list standard named filter). This approach lets you give the entry a sequence number.
- or, use this command to create an ACL and an ACL filter entry at the same time. With this approach, you cannot give the entry a sequence number, so the entry will go after any existing entries.

The **no** variant of this command removes a specified standard named access-list.

Syntax [to enter the sub-mode]

```
access-list standard <standard-acl-name>
no access-list standard <standard-acl-name>
```

Syntax [to create an ACL entry]

```
access-list standard <standard-acl-name> {deny|permit}
{any|<ip-addr>/<prefix>}
no access-list standard <standard-acl-name> {deny|permit}
{any|<ip-addr>/<prefix>}
```

Parameter	Description
<standard-acl-name>	Specify a name for the standard access-list.
deny	The access-list rejects packets that match the source filtering specified with this command.
permit	The access-list permits packets that match the source filtering specified with this command.
any	Match any source IP address.
<ip-addr>/<prefix>	Match the source address of the packets. Specify an IPv4 address in dotted decimal format, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes Use this command when configuring a standard named access-list for filtering IP software packets.

You can either create access-lists from within this command, or you can enter **access-list standard** followed by only the name. Entering only the name moves you to the IPv4 Standard ACL Configuration mode for the selected access-list. From

there you can configure your access-lists by using the command (access-list standard named filter).

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To define a standard access-list named 'my-list' and deny any packets from any source, use the commands:

```
awplus# configure terminal
awplus(config)# access-list standard my-list deny any
```

Alternatively, to define a standard access-list named 'my-list' and enter the IPv4 Standard ACL Configuration mode, and then create ACL entry 5 to deny any packets from any source, use the commands:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# 5 deny any
```

Related commands

(access-list standard named filter)

show running-config

show ip access-list

access-list (standard numbered)

Overview This command configures a standard numbered access-list that permits or denies packets from a specific source IP address. You can:

- use this command to enter a new or existing ACL number and enter the IPv4 Standard ACL Configuration mode. Once in that mode, you can create an ACL filter entry using the command (access-list standard numbered filter). This approach lets you give the entry a sequence number.
- or, use this command to create an ACL and an ACL filter entry at the same time. With this approach, you cannot give the entry a sequence number, so the entry will go after any existing entries.

The **no** variant of this command removes a specified standard numbered access-list.

Syntax [to enter the sub-mode]

```
access-list {<1-99>|<1300-1999>}
no access-list {<1-99>|<1300-1999>}
```

Syntax [to create an ACL entry]

```
access-list {<1-99>|<1300-1999>} {deny|permit} <source>
no access-list {<1-99>|<1300-1999>} {deny|permit} <source>
```

Parameter	Description	
<1-99>	IP standard access-list.	
<1300-1999>	IP standard access-list (expanded range).	
`deny`	Access-list rejects packets from the specified source.	
`permit`	Access-list accepts packets from the specified source.	
<source>	The source address of the packets. The following are the valid formats for specifying the source:	
	<ip-addr> <reverse-mask>	A source subnet, specified by entering the address and a reverse mask in dotted decimal format. For example, `192.168.1.0 0.0.0.255` (equivalent to 192.168.1.0/24).
	<ip-addr>	A single source address to match. The source address is specified in dotted decimal format.
	`host` *<ip-addr>*	A single source address to match. The source address is specified in dotted decimal format.
	`any`	Any source address.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes Use this command when configuring a standard numbered access-list for filtering IP software packets.

You can either create access-lists from within this command, or you can enter **access-list** followed by only the number. Entering only the number moves you to the IPv4 Standard ACL Configuration mode for the selected access-list. From there you can configure your access-lists by using the command (access-list standard numbered filter).

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To create ACL number 67 that will deny packets from subnet 172.16.10.0, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 67 deny 172.16.10.0 0.0.0.255
```

Alternatively, to define ACL number 67 and enter the IPv4 Standard ACL Configuration mode, and then create ACL entry 5 to deny any packets from subnet 172.16.10.0, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 67
awplus(config-ip-std-acl)# 5 deny 172.16.10.0 0.0.0.255
```

Related commands (access-list standard numbered filter)

show running-config

show ip access-list

(access-list standard named filter)

Overview This ACL filter adds a source IP address filter entry to a current named standard access-list. If the sequence number is specified, the new filter entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a source IP address filter entry from the current named standard access-list. You can specify the source IP address filter entry for removal by entering either its sequence number (e.g. **no 10**), or by entering its source IP address filter profile without specifying its sequence number (e.g. **no deny any**).

Note that you can find the sequence number by running the show access-list (IPv4 Software ACLs) command.

Syntax

```
[<sequence-number>] {deny|permit} {any|<ip-addr>/<prefix> [exact-match]}
no <sequence-number>
no {deny|permit} {any|<ip-addr>/<prefix> [exact-match]}
```

Parameter	Description
`<sequence-number>`	`<1-65535>` The sequence number for the filter entry of the selected access control list.
`deny`	Access-list rejects packets of the source filtering specified.
`permit`	Access-list allows packets of the source filtering specified
`any`	Match any source IP address.
`<ip-addr>/<prefix>`	Match the source address of the packets. Specify an IPv4 address in dotted decimal format, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
`exact-match`	Specify an exact IP prefix to match on.

Mode IPv4 Standard ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list standard (named) command with the required access control list name, but with no further parameters selected.*

Software ACLs will ***deny*** *access unless* ***explicitly permitted*** *by an ACL action.*

Examples

Use the following commands to add a new filter entry to access-list 'my-list' that will reject IP address 10.1.1.1:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# deny 10.1.1.1/32
```

Use the following commands to insert a new filter entry into access-list 'my-list' at sequence position number 15 that will accept IP network 10.1.2.0:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# 15 permit 10.1.2.0/24
```

Related commands

access-list standard (named)

show running-config

show ip access-list

(access-list standard numbered filter)

Overview This ACL filter adds a source IP address filter entry to a current standard numbered access-list. If a sequence number is specified, the new filter entry is inserted at the specified location. Otherwise, the new filter entry is added at the end of the access-list.

The **no** variant of this command removes a source IP address filter entry from the current standard numbered access-list. You can specify the source IP address filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its source IP address filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax

```
[<sequence-number>] {deny|permit} <source>
no {deny|permit} <source>
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets of the type specified.	
permit	Access-list allows packets of the type specified	
<source>	The source address of the packets. The following are the valid formats for specifying the source:	
	<ip-addr> <reverse-mask>	A source subnet, specified by entering the address and a reverse mask in dotted decimal format. For example, 192.168.1.0 0.0.0.255 (equivalent to 192.168.1.0/24).
	<ip-addr>	A single source address to match. The source address is specified in dotted decimal format.
	host *<ip-addr>*	A single source address to match. The source address is specified in dotted decimal format.
	any	Any source address.

Mode IPv4 Standard ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list (standard numbered) command with the required access control list number but with no further parameters selected.*

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example

To add a new entry accepting the IP network 10.1.1.0/24 at the sequence number 15 position, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 99
awplus(config-ip-std-acl)# 15 permit 10.1.2.0 0.0.0.255
```

Related commands

access-list (standard numbered)

show running-config

show ip access-list

clear ip prefix-list

Overview Use this command to reset the hit count to zero in the prefix-list entries.

Syntax

```
clear ip prefix-list [<list-name>] [<ip-address>/<mask>]
```

Parameter	Description
<list-name>	The name of the prefix-list.
<ip-address>/<mask>	The IP prefix and length.

Mode Privileged Exec

Example To clear a prefix-list named List1:

```
awplus# clear ip prefix-list List1
```

dos

Overview Use this command to configure Denial-of-Service (DoS) features for a port. Six different DoS attacks can be detected: IP Options, Land, Ping-of-Death, Smurf, Synflood and Teardrop.

When the attack is detected, three different actions are available:

- Shutdown the port for one minute
- Cause an SNMP trap.
- Send traffic to the mirror port

Syntax

```
dos {ipoptions|land|ping-of-death|smurf broadcast
<ip-address>|synflood|teardrop} action {shutdown|trap|mirror}
```

Parameter	Description
`dos`	Denial-Of-Service.
`ipoptions`	IP Options attack.
`land`	Land attack.
`ping-of-death`	Large ping attack.
`smurf`	Ping to broadcast address.
`broadcast`	Broadcast.
`<ip-address>`	Local IP Broadcast Address.
`synflood`	SYN flood attack.
`teardrop`	IP fragmentation attack.
`action`	Action.
`shutdown`	Shutdown port.
`trap`	Trap to SNMP.
`mirror`	Send packets to mirror port.

Mode Interface Configuration for a switch port interface.

Default DoS attack detection is not configured by default on any switch port interface.

Usage notes See the below table for more information about the DoS attacks recognized by this command:

Type of DoS attack	Description
ipoptions	This type of attack occurs when an attacker sends packets containing bad IP options to a victim node. There are many different types of IP options attacks and this software does not try to distinguish between them. Rather, if this defense is activated, the number of ingress IP packets containing IP options is counted. If the number exceeds 20 packets per second, the switch considers this a possible IP options attack. This defense does not require the CPU to monitor packets, so does not put extra load on the switch's CPU.
land	This type of attack occurs when the Source IP and Destination IP address are the same. This can cause a target host to be confused. Since packets with the same source and destination addresses should never occur, these packets are dropped when this attack is enabled. This defense does not require the CPU to monitor packets, so does not put extra load on the switch's CPU.
ping-of-death	This type of attack results from a fragmented packet which, when reassembled, would exceed the maximum size of a valid IP datagram. To detect this attack, the final fragment of ICMP packets has to be sent to the CPU for inspection. This defense can therefore load the CPU. Note that the extra CPU load will not affect normal traffic switching between ports, but other protocols such as IGMP and STP may be affected. This defense is not recommended where a large number of fragmented packets are expected.
smurf	This type of attack is an ICMP ping packet to a broadcast address. Although routers should not forward packets to local broadcast addresses anymore (see RFC2644), the Smurf attack can still be explicitly discarded with this command. In order for the Smurf attack to work, the broadcast IP address is required. Any ICMP Ping packet with this destination address is considered an attack. This defense does not require the CPU to monitor packets, so does not put extra load on the switch's CPU.
synflood	In this type of attack, an attacker, seeking to overwhelm a victim with TCP connection requests, sends a large number of TCP SYN packets with bogus source addresses to the victim. The victim responds with SYN ACK packets, but since the original source addresses are bogus, the victim node does not receive any replies. If the attacker sends enough requests in a short enough period, the victim may freeze operations once the requests exceed the capacity of its connections queue. To defend against this form of attack, a switch port monitors the number of ingress TCP-SYN packets it receives. An attack is recorded if a port receives more 60 TCP-SYN packets per second.
teardrop	In this DoS attack, an attacker sends a packet in several fragments with a bogus offset value, used to reconstruct the packet, in one of the fragments to a victim. This results in the victim being unable to reassemble the packet, possibly causing it to freeze operations.

Examples

To configure **smurf** DoS detection on port1.0.1, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos smurf broadcast 192.168.1.0 action shutdown
```

To configure **land** DoS detection on port1.0.1, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos land action shutdown
```

To configure **ipoptions** DoS detection on port1.0.1, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos ipoptions action shutdown
```

To configure **ping-of-death** DoS detection on port1.0.1, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos ping-of-death action shutdown
```

To configure **synflood** DoS detection on port1.0.1, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos synflood action shutdown
```

To configure **teardrop** DoS detection on port1.0.1, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos teardrop action shutdown
```

Related commands

show dos interface

ip prefix-list

Overview Use this command to create an entry for an IPv4 prefix list.

Use the **no** variant of this command to delete the IPv4 prefix-list entry.

Syntax

```
ip prefix-list <list-name> [seq <1-429496725>] {deny|permit}
{any|<ip-prefix>} [ge <0-32>] [le <0-32>]
ip prefix-list <list-name> description <text>
ip prefix-list sequence-number
no ip prefix-list <list-name> [seq <1-429496725>]
no ip prefix-list <list-name> [description <text>]
no ip prefix-list sequence-number
```

Parameter	Description
<list-name>	Specifies the name of a prefix list.
seq *<1-429496725>*	Sequence number of the prefix list entry.
deny	Specifies that the prefixes are excluded from the list.
permit	Specifies that the prefixes are included in the list.
<ip-prefix>	Specifies the IPv4 address and length of the network mask in dotted decimal in the format A.B.C.D/M.
any	Any prefix match. Same as **0.0.0.0/0 le 32**.
ge*<0-32>*	Specifies the minimum prefix length to be matched.
le*<0-32>*	Specifies the maximum prefix length to be matched.
<text>	Text description of the prefix list.
sequence-number	Specify sequence numbers included or excluded in prefix list.

Mode Global Configuration

Usage notes When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the **seq** parameter and place common permits or denials towards the top of the list. If you do not use the **seq** parameter, the sequence values are generated in a sequence of 5.

The parameters **ge** and **le** specify the range of the prefix lengths to be matched. When setting these parameters, set the **le** value to be less than 32, and the **ge** value to be less than or equal to the **le** value and greater than the ip-prefix mask length.

Prefix lists implicitly exclude prefixes that are not explicitly permitted in the prefix list. This means if a prefix that is being checked against the prefix list reaches the end of the prefix list without matching a permit or deny, this prefix will be denied.

Example In the following sample configuration, the last **ip prefix-list** command in the below list matches all, and the first **ip prefix-list** command denies the IP network 76.2.2.0:

```
awplus(config)# router bgp 100
awplus(config-router)# network 172.1.1.0
awplus(config-router)# network 172.1.2.0
awplus(config-router)# neighbor 10.6.5.3 remote-as 300
awplus(config-router)# neighbor 10.6.5.3 prefix-list mylist out
awplus(config-router)# exit
awplus(config)# ip prefix-list mylist seq 5 deny 76.2.2.0/24
awplus(config)# ip prefix-list mylist seq 100 permit any
```

To deny the IP addresses between 10.0.0.0/14 (10.0.0.0 255.252.0.0) and 10.0.0.0/22 (10.0.0.0 255.255.252.0) within the 10.0.0.0/8 (10.0.0.0 255.0.0.0) addressing range, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip prefix-list mylist seq 12345 deny 10.0.0.0/8
ge 14 le 22
```

Related commands

match ip address

neighbor prefix-list

area filter-list

clear ip prefix-list

match route-type

show ip prefix-list

maximum-access-list (deleted)

Overview This command has been removed from version 5.5.1-01 onwards. There is no alternative command.

show access-list (IPv4 Software ACLs)

Overview Use this command to display the specified access-list, or all access-lists if none have been specified. Note that only defined access-lists are displayed. An error message is displayed for an undefined access-list

Syntax

```
show access-list
[<1-99>|<100-199>|<1300-1999>|<2000-2699>|<3000-3699>|
<4000-4499>|<access-list-name>]
```

Parameter	Description
<1-99>	IP standard access-list.
<100-199>	IP extended access-list.
<1300-1999>	IP standard access-list (standard - expanded range).
<2000-2699>	IP extended access-list (extended - expanded range).
<3000-3699>	Hardware IP access-list.
<4000-4499>	Hardware MAC access-list.
<access-list-name>	IP named access-list.

Mode User Exec and Privileged Exec

Examples To show all access-lists configured on the switch:

```
awplus# show access-list
```

```
Standard IP access list 1
    deny 172.16.2.0, wildcard bits 0.0.0.255
Standard IP access list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
Hardware IP access list 3001
    permit ip 192.168.20.0 255.255.255.0 any
Hardware IP access list 3020
    permit tcp any 192.0.2.0/24
awplus#show access-list 20
```

To show the access-list with an ID of 20:

```
awplus# show access-list 20
```

```
Standard IP access-list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
```

Note the following error message is displayed if you attempt to show an undefined access-list:

```
awplus# show access-list 2
```

```
% Can't find access-list 2
```

Related commands

access-list standard (named)

access-list (standard numbered)

access-list (extended numbered)

show dos interface

Overview Use this command to display the Denial-of-Service (DoS) features configured on a switch port interface from the dos command. See the dos command for descriptions of DoS attack types.

Syntax `show dos interface {<port-list>}`

Parameter	Description
<port-list>	Specify the switch port or port list to display DoS configuration options set with the dos command.

Mode Privileged Exec

Output Figure 39-1: Example output from the **show dos interface** command prior to a DoS attack

```
awplus#configure terminal
Enter configuration commands, one per line. End with CTNTL/Z.
awplus(config)#interface port1.0.1
awplus(config-if)#dos synflood action shutdown
awplus(config-if)#exit
awplus(config)#exit
awplus#show dos interface port1.0.1

DoS settings  for interface port1.0.1
----------------------------------------
Port status          : Enabled
ipoptions            : Disabled
land                 : Disabled
ping-of-death        : Disabled
smurf                : Disabled
synflood             : Enabled
   Action            : Shutdown port
   Attacks detected  : 0
teardrop             : Disabled
awplus#
```

Figure 39-2: Example output from the **show dos interface** command after a **synflood** DoS attack

```
awplus#show dos interface port1.0.1

DoS settings for interface port1.0.1
----------------------------------------
Port status          : Enabled
ipoptions            : Disabled
land                 : Disabled
ping-of-death        : Disabled
smurf                : Disabled
synflood             : Enabled
   Action            : Shutdown port
   Attacks detected  : 1
teardrop             : Disabled
awplus#
```

Table 40: Parameters in the **show dos interface** command output:

Type of DoS attack	Description
`Port status`	Displays `Enabled` when the port is configured as being administratively up after issuing the **no shutdown** command. Displays `Disabled` when the port is configured as being administratively down with the **shutdown** command.
`ipoptions`	Displays `Enabled` when the **ipoptions** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **ipoptions** DoS attacks that have occurred on the interface. Displays `Disabled` when the **ipoptions** parameter is not configured with the dos command.
`land`	Displays `Enabled` when the **land** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **land** DoS attacks that have occurred on the interface. Displays `Disabled` when the **land** parameter is not configured with the dos command.
`ping-of-death`	Displays `Enabled` when the **ping-of-death** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **ping-of-death** DoS attacks that have occurred on the interface. Displays `Disabled` when the **ping-of-death** parameter is not configured with the dos command.

Table 40: Parameters in the **show dos interface** command output: (cont.)

Type of DoS attack	Description
`smurf`	Displays `Enabled` when the **smurf** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **smurf** DoS attacks that have occurred on the interface. Displays `Disabled` when the **smurf** parameter is not configured with the dos command.
`synflood`	Displays `Enabled` when the **synflood** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **synflood** DoS attacks that have occurred on the interface. Displays `Disabled` when the **synflood** parameter is not configured with the dos command.
`teardrop`	Displays `Enabled` when the **teardrop** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **teardrop** DoS attacks that have occurred on the interface. Displays `Disabled` when the **teardrop** parameter is not configured with the dos command.

Related commands dos

show ip access-list

Overview Use this command to display IP access-lists.

Syntax
```
show ip access-list
[<1-99>|<100-199>|<1300-1999>|<2000-2699>|<access-list-name>]
```

Parameter	Description
<1-99>	IP standard access-list.
<100-199>	IP extended access-list.
<1300-1999>	IP standard access-list (expanded range).
<2000-2699>	IP extended access-list (expanded range).
<access-list-name>	IP named access-list.

Mode User Exec and Privileged Exec

Example
```
awplus# show ip access-list
```

Output Figure 39-3: Example output from the **show ip access-list** command

```
Standard IP access-list 1
    permit 172.168.6.0, wildcard bits 0.0.0.255
    permit 192.168.6.0, wildcard bits 0.0.0.255
```

show ip prefix-list

Overview Use this command to display the IPv4 prefix-list entries.

Note that this command is valid for RIP and BGP routing protocols only.

Syntax

```
show ip prefix-list [<name>|detail|summary]
```

Parameter	Description
<name>	Specify the name of a prefix list in this placeholder.
`detail`	Specify this parameter to show detailed output for all IPv4 prefix lists.
`summary`	Specify this parameter to show summary output for all IPv4 prefix lists.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip prefix-list
awplus# show ip prefix-list 10.10.0.98/8
awplus# show ip prefix-list detail
```

Related commands ip prefix-list

vty access-class (numbered)

Overview For IPv4, use this command to set a standard numbered software access list to be the management ACL. This is then applied to all available VTY lines for controlling remote access by Telnet and SSH. This command allows or denies packets containing the IP addresses included in the ACL to create a connection to your device.

ACLs that are attached using this command have an implicit deny-all filter as the final entry in the ACL. So a typical configuration would be to permit a specific address, or range of addresses, and rely on the deny-all filter to block all other access.

Use the **no** variant of this command to remove the access list.

Syntax

```
vty access-class {<1-99>|<1300-1999>}
no vty access-class [<1-99>|<1300-1999>]
```

Parameter	Description
<1-99>	IPv4 standard access-list number
<1300-1999>	IPv4 standard access-list number (expanded range)

Mode Global Configuration

Examples To set access-list 4 to be the management ACL, use the following commands:

```
awplus# configure terminal
awplus(config)# vty access-class 4
```

To remove access-list 4 from the management ACL, use the following commands:

```
awplus# configure terminal
awplus(config)# no vty access-class 4
```

Output Figure 39-4: Example output from the **show running-config** command

```
awplus#show running-config|grep access-class

vty access-class 4
```

Related commands

show running-config

vty ipv6 access-class (named)

40 IPv6 Hardware Access Control List (ACL) Commands

Introduction

Overview This chapter provides an alphabetical reference for the IPv6 Hardware Access Control List (ACL) commands, and contains detailed command information and command examples about IPv6 hardware ACLs, which are applied directly to interfaces using the ipv6 traffic-filter command.

For information about ACLs, see the ACL Feature Overview and Configuration Guide.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see the following references:

- Link Aggregation Feature Overview_and_Configuration_Guide.
- Link Aggregation Commands

Most ACL command titles include usage information in parentheses. When the command title is completely surrounded by parentheses, the title indicates the type of ACL filter instead of keywords to enter into the CLI. For example, the title **(named IPv6 hardware ACL: IP protocol entry)** represents a command with the syntax:

```
[<sequence-number>] <action> proto <1-255> <source-addr>
<dest-addr> [vlan <1-4094>]
```

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Sub-modes Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 40-1: IPv6 Hardware Access List Commands and Prompts

Command Name	Command Mode	Prompt
show acl-group ipv6 address	Privileged Exec	awplus#
show ipv6 access-list (IPv6 Hardware ACLs)	Privileged Exec	awplus#
acl-group ipv6 address	Global Configuration	awplus(config)#
ipv6 access-list (named IPv6 hardware ACL)	Global Configuration	awplus(config)#
ipv6 traffic-filter	Interface Configuration	awplus(config-if)#
commit (IPv6)	IPv6 Hardware ACL Configuration	awplus(config-ipv6-hw-acl)#
(named IPv6 hardware ACL: IPv6 packet entry)	IPv6 Hardware ACL Configuration	awplus(config-ipv6-hw-acl)#
(named IPv6 hardware ACL: ICMP entry)	IPv6 Hardware ACL Configuration	awplus(config-ipv6-hw-acl)#
(named IPv6 hardware ACL: IP protocol entry)	IPv6 Hardware ACL Configuration	awplus(config-ipv6-hw-acl)#
(named IPv6 hardware ACL: TCP or UDP entry)	IPv6 Hardware ACL Configuration	awplus(config-ipv6-hw-acl)#
ipv6 (ipv6-host-group)	IPv6 ACL Host Group Configuration	awplus(config-ipv6-host-group)#

Command List

- "acl-group ipv6 address" on page 2016
- "commit (IPv6)" on page 2017
- "ipv6 (ipv6-host-group)" on page 2018
- "ipv6 access-list (named IPv6 hardware ACL)" on page 2020
- "ipv6 traffic-filter" on page 2022
- "(named IPv6 hardware ACL: ICMP entry)" on page 2023
- "(named IPv6 hardware ACL: IPv6 packet entry)" on page 2027
- "(named IPv6 hardware ACL: IP protocol entry)" on page 2030
- "(named IPv6 hardware ACL: TCP or UDP entry)" on page 2035
- "show acl-group ipv6 address" on page 2039
- "show ipv6 access-list (IPv6 Hardware ACLs)" on page 2040

acl-group ipv6 address

Overview Use this command to create a new named IPv6 ACL group that contains one or more IPv6 host or subnets.

This command creates a named IPv6 ACL group and enters the ACL Host Group config mode. IPv6 hosts or subnets can be added to or removed from this group. This host group can be used as a source or destination match for any hardware ACL to simplify large ACL configs with lots of IPv6 hosts.

Use the **no** variant of this command to delete an IPv6 ACL group.

Syntax

```
acl-group ipv6 address <group>
no acl-group ipv6 address <group>
```

Parameter	Description
<group>	The name of the IPv6 ACL group.

Default No ACL groups exist by default.

Mode Global Configuration

Example To create an IPv6 ACL group named IPV6 _GROUP1, use the commands:

```
awplus# configure terminal
awplus(config)# acl-group ipv6 address IPV6_GROUP1
awplus(config-ip-host-group)#
```

To delete an IPv6 ACL group named IPVv6 _GROUP1, use the commands:

```
awplus# configure terminal
awplus(config)# no acl-group ipv6 address IPV6_GROUP1
```

Related commands ipv6 (ipv6-host-group)

show acl-group ipv6 address

Command changes Version 5.5.0-1.1: command added

commit (IPv6)

Overview Use this command to commit the IPv6 ACL filter configuration entered at the console to the hardware immediately without exiting the IPv6 Hardware ACL Configuration mode.

This command forces the associated hardware and software IPv6 ACLs to synchronize.

Syntax

```
commit
```

Mode IPv6 Hardware ACL Configuration

Usage notes Normally, when an IPv6 hardware ACL is edited, the new configuration state of the IPv6 ACL is not written to hardware until you exit IPv6 Hardware ACL Configuration mode. By entering this command you can ensure that the current state of a hardware access-list that is being edited is written to hardware immediately.

Scripts typically do not include the exit command to exit configuration modes, potentially leading to IPv6 ACL filters in hardware not being correctly updated. Using this **commit** command in a configuration script after specifying an IPv6 hardware ACL filter ensures that it is updated in the hardware.

Example To update the hardware with the IPv6 ACL filter configuration, use the command:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-ipv6-acl
awplus(config-ipv6-hw-acl)# commit
```

Related commands ipv6 access-list (named IPv6 hardware ACL)

ipv6 (ipv6-host-group)

Overview Use this command to add an IPv6 host or subnet to an IPv6 ACL group. Adding IPv6 hosts and subnets to an ACL group allows you to simplify ACL config when the same IP addresses are required for many ACLs.

Use the **no** variant of this command to remove an IPv6 host or subnet from an IPv6 ACL group.

Syntax

```
ipv6 {any|<match-ip>}
no ipv6 {any|<match-ip>}
```

Parameter	Description	
`any`	Match any IP address.	
<match-ip>	The addresses to match against. You can specify a single host or a subnet. The following are the valid formats for specifying the addresses:	
	<ipv6-addr>	Specifies a single host address. The IPv6 address uses the format X:X::X:X.
	<ipv6-addr>/<prefix>	Specifies an address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64, or has the value 128.
	<ipv6-addr> <reverse-mask>	An IPv6 host and a reverse mask in format X:X::X:X.

Default No hosts or subnets are in an IPv6 ACL group by default.

Mode IPv6 ACL Host Group Configuration

Example To add the subnet 2001:DB8::/32 to an IPv6 ACL group IPV6_GROUP1, use the commands:

```
awplus# configure terminal
awplus(config)# acl-group ipv6 address IPV6_GROUP1
awplus(config-ipv6-host-group)# ipv6 2001:DB8::/32
```

To remove the subnet 2001:DB8::/32 from an IPv6 ACL group IPV6_GROUP1, use the commands:

```
awplus# configure terminal
awplus(config)# acl-group ipv6 address IPV6_GROUP1
awplus(config-ipv6-host-group)# no ipv6 2001:DB8::/32
```

Related commands

acl-group ipv6 address

show acl-group ipv6 address

Command changes

Version 5.5.0-1.1: command added

ipv6 access-list (named IPv6 hardware ACL)

Overview Use this command to either create a new IPv6 hardware access-list, or to select an existing IPv6 hardware access-list in order to apply a filter entry to it.

Use the **no** variant of this command to delete an existing IPv6 hardware access-list.

NOTE: *Before you can delete an access-list, you must first remove it from any interface it is assigned to.*

Syntax

```
ipv6 access-list <ipv6-access-list-name>
no ipv6 access-list <ipv6-access-list-name>
```

Parameter	Description
<ipv6-access-list-name>	Specify an IPv6 access-list name.

Mode Global Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage notes Use IPv6 hardware named access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 hardware named access-list when a match is encountered.

This command moves you to the (config-ipv6-hw-acl) prompt for the selected IPv6 hardware named access-list number. From there you can configure the filters for this selected IPv6 hardware named access-list.

Once you have configured the ACL, use the ipv6 traffic-filter or the match access-group command to apply this ACL to a port, VLAN or QoS class-map. Note that the ACL will only apply to incoming data packets.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

Examples To create an IPv6 access-list named “my-ipv6-acl”, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-ipv6-acl
awplus(config-ipv6-hw-acl)#
```

To delete the IPv6 access-list named “my-ipv6-acl”, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 access-list my-ipv6-acl
```

Related commands (named IPv6 hardware ACL: ICMP entry)

(named IPv6 hardware ACL: IPv6 packet entry)

(named IPv6 hardware ACL: IP protocol entry)

(named IPv6 hardware ACL: TCP or UDP entry)

ipv6 traffic-filter

match access-group

show ipv6 access-list (IPv6 Hardware ACLs)

ipv6 traffic-filter

Overview This command adds an IPv6 hardware-based access-list to an interface. The number of access-lists that can be added is determined by the amount of available space in the hardware-based packet classification tables.

Use the **no** variant of this command to remove an IPv6 hardware-based access-list from an interface.

Syntax

```
ipv6 traffic-filter <ipv6-access-list-name>
no ipv6 traffic-filter <ipv6-access-list-name>
```

Parameter	Description
<ipv6-access-list-name>	Hardware IPv6 access-list name.

Mode Interface Configuration (to apply an IPv6 hardware ACL to a specific switch port).

Usage notes This command adds an IPv6 hardware-based access-list to an interface. The number of access-lists that can be added is determined by the amount of available space in the hardware-based packet classification tables.

Examples To add access-list “acl1” as a traffic-filter to interface port1.0.1, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# ipv6 traffic-filter acl1
```

To remove access-list “acl1” as a traffic-filter from interface port1.0.1, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no ipv6 traffic-filter acl1
```

Related commands

ipv6 access-list (named IPv6 hardware ACL)

(named IPv6 hardware ACL: ICMP entry)

(named IPv6 hardware ACL: IPv6 packet entry)

(named IPv6 hardware ACL: IP protocol entry)

(named IPv6 hardware ACL: TCP or UDP entry)

show ipv6 access-list (IPv6 Hardware ACLs)

(named IPv6 hardware ACL: ICMP entry)

Overview

Use this command to add a new ICMP filter entry to the current IPv6 hardware access-list. The filter will match on any ICMP packet that has the specified IPv6 source and destination IP addresses and (optionally) ICMP type. You can specify the value **any** if source or destination address does not matter.

The **no** variant of this command removes a filter entry from the current IPv6 hardware access-list. You can specify the filter entry for removal by entering either its sequence number (e.g. **no 100**), or by entering its filter profile without specifying its sequence number (e.g. **no deny icmp 2001:0db8::0/64 any**).

You can find the sequence number by running the show ipv6 access-list (IPv6 Hardware ACLs) command.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
[<sequence-number>] <action> icmp <source-addr> <dest-addr>
[icmp-type <number>] [vlan <1-4094>]
```

```
no <sequence-number>
```

```
no <action> icmp <source-addr> <dest-addr> [icmp-type <number>]
[vlan <1-4094>]
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Parameter	Description	
<sequence-number>	The sequence number for the filter entry of the selected access control list, in the range 1-65535.	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
icmp	Match against ICMP packets	
<source-addr>	The source addresses to match against. You can specify a single host, a range, or all source addresses. The following are the valid formats for specifying the source:	
	any	Match any source host.
	<ipv6-src-address/prefix-length>	Match the specified source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
	<ipv6-src-address> *<ipv6-src-wildcard>*	Match the specified IPv6 source address, masked using wildcard bits. The IPv6 address uses the format X:X::X:X. In the wildcard bits, 1 represents bits to ignore, and 0 represents bits to match
	host *<ipv6-source-host>*	Match a single source host address. The IPv6 address uses the format X:X::X:X.
<dest-addr>	The destination addresses to match against. You can specify a single host, a range, or all destination addresses. The following are the valid formats for specifying the destination:	
	any	Match any destination host.
	<ipv6-dest-address/prefix-length>	Match the specified destination address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
	<ipv6-dest-address> *<ipv6-dest-wildcard>*	Match the specified destination address, masked using wildcard bits. The IPv6 address uses the format X:X::X:X. In the wildcard bits, 1 represents bits to ignore, and 0 represents bits to match

Parameter	Description	
	`host <ipv6-dest-host>`	Match a single destination host address. The IPv6 address uses the format X:X::X:X.
`icmp-type <number>`	The type of ICMP message to match against, as defined in RFC792 and RFC950. Values include:	
	0	Echo replies.
	3	Destination unreachable messages.
	4	Source quench messages.
	5	Redirect (change route) messages.
	8	Echo requests.
	11	Time exceeded messages.
	12	Parameter problem messages.
	13	Timestamp requests.
	14	Timestamp replies.
	15	Information requests.
	16	Information replies.
	17	Address mask requests.
	18	Address mask replies.
`vlan <1-4094>`	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Mode IPv6 Hardware ACL Configuration (accessed by running the command ipv6 access-list (named IPv6 hardware ACL))

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes To use this command, first run the command ipv6 access-list (named IPv6 hardware ACL) and enter the desired access-list name. This changes the prompt to awplus(config-ipv6-hw-acl)#.

Then use this command (and the other "named IPv6 hardware ACL: entry" commands) to add filter entries. You can add multiple filter entries to an ACL.

If you specify a sequence number, the new entry is inserted at the specified location. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number.

Once you have configured the ACL, use the ipv6 traffic-filter or the match access-group command to apply this ACL to a port, VLAN or QoS class-map. Note that the ACL will only apply to incoming data packets.

Examples

To add a filter entry to the ACL named "my-acl", to block ICMP packets sent from network 2001:0db8::0/64 , use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny icmp 2001:0db8::0/64 any
```

To remove a filter entry from the ACL named "my-acl" that blocks all ICMP packets sent from network 2001:0db8::0/ 64 , use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# no deny icmp 2001:0db8::0/64 any
```

To specify an ACL named "my-acl1" and add a filter entry that blocks all ICMP6 echo requests, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl1
awplus(config-ipv6-hw-acl)# deny icmp any any icmp-type 128
```

To specify an ACL named "my-acl2" and add a filter entry that blocks all ICMP6 echo requests on the default VLAN (vlan1), enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl2
awplus(config-ipv6-hw-acl)# deny icmp any any icmp-type 128
vlan 1
```

To remove a filter entry that blocks all ICMP6 echo requests from the ACL named "my-acl1", enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl1
awplus(config-ipv6-hw-acl)# no deny icmp any any icmp-type 128
```

Related commands

ipv6 access-list (named IPv6 hardware ACL)

ipv6 traffic-filter

match access-group

show ipv6 access-list (IPv6 Hardware ACLs)

(named IPv6 hardware ACL: IPv6 packet entry)

Overview

Use this command to add an IPv6 packet filter entry to the current hardware access-list. The filter will match on IPv6 packets that have the specified source and destination IPv6 address and (optionally) prefix. You can use the value **any** instead of source or destination IPv6 address if an address does not matter.

The **no** variant of this command removes a filter entry from the current hardware access-list. You can specify the filter entry for removal by entering either its sequence number (e.g. **no 100**), or by entering its filter profile without specifying its sequence number (e.g. **no deny ipv6 2001:0db8::0/64 any**).

You can find the sequence number by running the show ipv6 access-list (IPv6 Hardware ACLs) command.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
[<sequence-number>] <action> ipv6 <source-addr> <dest-addr>
[vlan <1-4094>]
```

```
no <sequence-number>
```

```
no <action> ipv6 <source-addr> <dest-addr> [vlan <1-4094>]
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Parameter	Description	
<sequence-number>	The sequence number for the filter entry of the selected access control list, in the range 1-65535.	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
ipv6	Match against IPv6 packets	
<source-addr>	The source addresses to match against. You can specify a single host, a range, or all source addresses. The following are the valid formats for specifying the source:	
	any	Match any source host.
	<ipv6-src-address/prefix-length>	Match the specified source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
	<ipv6-src-address> *<ipv6-src-wildcard>*	Match the specified IPv6 source address, masked using wildcard bits. The IPv6 address uses the format X:X::X:X. In the wildcard bits, 1 represents bits to ignore, and 0 represents bits to match
	host *<ipv6-source-host>*	Match a single source host address. The IPv6 address uses the format X:X::X:X.
<dest-addr>	The destination addresses to match against. You can specify a single host, a range, or all destination addresses. The following are the valid formats for specifying the destination:	
	any	Match any destination host.
	<ipv6-dest-address/prefix-length>	Match the specified destination address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
	<ipv6-dest-address> *<ipv6-dest-wildcard>*	Match the specified destination address, masked using wildcard bits. The IPv6 address uses the format X:X::X:X. In the wildcard bits, 1 represents bits to ignore, and 0 represents bits to match

Parameter	Description	
	`host <ipv6-dest-host>`	Match a single destination host address. The IPv6 address uses the format X:X::X:X.
`vlan <1-4094>`	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Mode IPv6 Hardware ACL Configuration (accessed by running the command ipv6 access-list (named IPv6 hardware ACL))

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes To use this command, first run the command ipv6 access-list (named IPv6 hardware ACL) and enter the desired access-list name. This changes the prompt to awplus(config-ipv6-hw-acl)#.

Then use this command (and the other "named IPv6 hardware ACL: entry" commands) to add filter entries. You can add multiple filter entries to an ACL.

If you specify a sequence number, the new entry is inserted at the specified location. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number.

Once you have configured the ACL, use the ipv6 traffic-filter or the match access-group command to apply this ACL to a port, VLAN or QoS class-map. Note that the ACL will only apply to incoming data packets.

Examples To add a filter entry to the ACL named "my-acl" to block IPv6 traffic sent from network 2001:0db8::0/64, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny ipv6 2001:0db8::0/64 any
```

To remove a filter entry from the ACL named "my-acl" that blocks all IPv6 traffic sent from network 2001:0db8::0/ 64, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# no deny ipv6 2001:0db8::0/64 any
```

Related commands ipv6 access-list (named IPv6 hardware ACL)

ipv6 traffic-filter

match access-group

show ipv6 access-list (IPv6 Hardware ACLs)

(named IPv6 hardware ACL: IP protocol entry)

Overview

Use this command to add an IP protocol type filter entry to the current IPv6 hardware access-list. The filter will match on IPv6 packets that have the specified IP protocol number, and the specified IPv6 addresses. You can use the value **any** instead of source or destination IPv6 address if an address does not matter.

The **no** variant of this command removes a filter entry from the current hardware access-list. You can specify the filter entry for removal by entering either its sequence number (e.g. **no 100**), or by entering its filter profile without specifying its sequence number (e.g. **no deny proto 2 2001:0db8::0/64 any**).

You can find the sequence number by running the show ipv6 access-list (IPv6 Hardware ACLs) command.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
[<sequence-number>] <action> proto <1-255> <source-addr>
<dest-addr> [vlan <1-4094>]

no <sequence-number>

no <action> proto <1-255> <source-addr> <dest-addr> [vlan
<1-4094>]
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Table 40-2: Parameters in IP protocol ACL entries

Parameter	Description	
<sequence-number>	The sequence number for the filter entry of the selected access control list, in the range 1-65535.	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
proto *<1-255>*	The IP protocol number to match against, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.	
<source-addr>	The source addresses to match against. You can specify a single host, a range, or all source addresses. The following are the valid formats for specifying the source:	
	any	Match any source host.
	<ipv6-src-address/prefix-length>	Match the specified source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
	<ipv6-src-address> *<ipv6-src-wildcard>*	Match the specified IPv6 source address, masked using wildcard bits. The IPv6 address uses the format X:X::X:X. In the wildcard bits, 1 represents bits to ignore, and 0 represents bits to match
	host *<ipv6-source-host>*	Match a single source host address. The IPv6 address uses the format X:X::X:X.
<dest-addr>	The destination addresses to match against. You can specify a single host, a range, or all destination addresses. The following are the valid formats for specifying the destination:	
	any	Match any destination host.
	<ipv6-dest-address/prefix-length>	Match the specified destination address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.

Table 40-2: Parameters in IP protocol ACL entries (cont.)

Parameter	Description	
	<ipv6-dest-address> *<ipv6-dest-wildcard>*	Match the specified destination address, masked using wildcard bits. The IPv6 address uses the format X:X::X:X. In the wildcard bits, 1 represents bits to ignore, and 0 represents bits to match
	host *<ipv6-dest-host>*	Match a single destination host address. The IPv6 address uses the format X:X::X:X.
vlan *<1-4094>*	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Table 40-3: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]

Table 40-3: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode IPv6 Hardware ACL Configuration (accessed by running the command ipv6 access-list (named IPv6 hardware ACL))

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes To use this command, first run the command ipv6 access-list (named IPv6 hardware ACL) and enter the desired access-list name. This changes the prompt to awplus(config-ipv6-hw-acl)#.

Then use this command (and the other “named IPv6 hardware ACL: entry” commands) to add filter entries. You can add multiple filter entries to an ACL.

If you specify a sequence number, the new entry is inserted at the specified location. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number.

Once you have configured the ACL, use the ipv6 traffic-filter or the match access-group command to apply this ACL to a port, VLAN or QoS class-map. Note that the ACL will only apply to incoming data packets.

Examples

To add a filter entry to the ACL named "my-acl" to deny IGMP packets from 2001:0db8::0/64 , use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny proto 2 2001:0db8::0/64 any
```

To remove a filter entry that blocks IGMP packets from network 2001:0db8::0/64 from the ACL named "my-acl", use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# no deny proto 2 2001:0db8::0/64 any
```

Related commands

ipv6 access-list (named IPv6 hardware ACL)

ipv6 traffic-filter

match access-group

show ipv6 access-list (IPv6 Hardware ACLs)

(named IPv6 hardware ACL: TCP or UDP entry)

Overview Use this command to add a TCP or UDP filter entry to the current IPv6 hardware access-list. The access-list will match on TCP or UDP packets that have the specified source and destination IP addresses and optionally, port values. You can use the value **any** instead of source or destination IP address if an address does not matter.

The **no** variant of this command removes a filter entry from the current hardware access-list. You can specify the filter entry for removal by entering either its sequence number (e.g. **no 100**), or by entering its filter profile without specifying its sequence number (e.g. **no deny tcp 2001:0db8::0/64 any**).

You can find the sequence number by running the show ipv6 access-list (IPv6 Hardware ACLs) command.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

CAUTION: *Specifying a "send" action enables you to use ACLs to redirect packets from their original destination. Use such ACLs with caution. They could prevent control packets from reaching the correct destination, such as EPSR healthcheck messages and AMF messages.*

Syntax

```
[<sequence-number>] <action> {tcp|udp} <source-addr>
[<source-ports>] <dest-addr> [<dest-ports>] [vlan <1-4094>]

no <sequence-number>

no <action> {tcp|udp} <source-addr> [<source-ports>]
<dest-addr> [<dest-ports>] [vlan <1-4094>]
```

The following actions are available for hardware ACLs:

Values for the <action> parameter	
`deny`	Reject packets that match the source and destination filtering specified with this command.
`permit`	Permit packets that match the source and destination filtering specified with this command.
`copy-to-cpu`	Send a copy of matching packets to the CPU.
`copy-to-mirror`	Send a copy of matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-mirror`	Send matching packets to the mirror port. Use the **mirror interface** command to configure the mirror port.
`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.
`send-to-cpu`	Send matching packets to the CPU.

Parameter	Description	
<sequence-number>	The sequence number for the filter entry of the selected access control list, in the range 1-65535. If you do not specify a sequence number, the switch puts the entry at the end of the ACL and assigns it the next available multiple of 10 as its sequence number. .	
<action>	The action that the switch will take on matching packets. See the table above for valid values.	
`tcp`	Match against TCP packets.	
`udp`	Match against UDP packets.	
<source-addr>	The source addresses to match against. You can specify a single host, a subnet, or all source addresses. The following are the valid formats for specifying the source:	
	`any`	Match any source IP address.
	`host` *<ip-addr>*	Match a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	Match any source IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> *<reverse-mask>*	Match any source IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<source-ports>	Match source TCP or UDP port numbers. Port numbers are specified as integers between 0 and 65535. You can specify one or more port numbers as follows:	
	`eq <0-65535>`	Match a single port number.
	`lt <0-65535>`	Match all port numbers that are less than the specified port number.
	`gt <0-65535>`	Match all port numbers that are greater than the specified port number.
	`ne <0-65535>`	Match all port numbers except the specified port number.
	`range` *<start-port>* *<end-port>*	Match a range of port numbers.
<dest-addr>	The destination addresses to match against. You can specify a single host, a subnet, or all destination addresses. The following are the valid formats for specifying the destination:	

Parameter	Description	
	`any`	Match any destination IP address.
	`host <ip-addr>`	Match a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/ *<prefix>*	Match any destination IP address within the specified subnet. Specify the subnet by entering the IPv4 address, then a forward slash, then the prefix length.
	<ip-addr> *<reverse-mask>*	Match any destination IP address within the specified subnet. Specify the subnet by entering a reverse mask in dotted decimal format. For example, entering "192.168.1.1 0.0.0.255" is the same as entering 192.168.1.1/24.
<dest-ports>	Match destination TCP or UDP port numbers. Port numbers are specified as integers between 0 and 65535. You can specify one or more port numbers as follows:	
	`eq <0-65535>`	Match a single port number.
	`lt <0-65535>`	Match all port numbers that are less than the specified port number.
	`gt <0-65535>`	Match all port numbers that are greater than the specified port number.
	`ne <0-65535>`	Match all port numbers except the specified port number.
	`range <start-port> <end-port>`	Match a range of port numbers.
`vlan <1-4094>`	The VLAN to match against. The ACL will match against the specified ID in the packet's VLAN tag.	

Mode IPv6 Hardware ACL Configuration (accessed by running the command ipv6 access-list (named IPv6 hardware ACL))

Default On an interface controlled by a hardware ACL, any traffic that does not explicitly match a filter is permitted.

Usage notes To use this command, first run the command ipv6 access-list (named IPv6 hardware ACL) and enter the desired access-list name. This changes the prompt to awplus(config-ipv6-hw-acl)#.

Then use this command (and the other "named IPv6 hardware ACL: entry" commands) to add filter entries. You can add multiple filter entries to an ACL.

If you specify a sequence number, the new entry is inserted at the specified location. If you do not specify a sequence number, the switch puts the entry at the

end of the ACL and assigns it the next available multiple of 10 as its sequence number.

Once you have configured the ACL, use the ipv6 traffic-filter or the match access-group command to apply this ACL to a port, VLAN or QoS class-map. Note that the ACL will only apply to incoming data packets.

Examples

To add a filter entry that blocks all SSH traffic from network 2001:0db8::0/64 to the hardware IPv6 access-list named "my-acl", use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny tcp 2001:0db8::0/64 any eq 22
```

To add a filter entry that blocks all SSH traffic from network 2001:0db8::0/64 on the default VLAN (vlan1) to the hardware IPv6 access-list named "my-acl", use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny tcp 2001:0db8::0/64 any eq 22
vlan 1
```

To remove an ACL filter entry that blocks all SSH traffic from network 2001:0db8::0/64 from the hardware IPv6 access-list named "my-acl", use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# no deny tcp 2001:0db8::0/64 any eq
22
```

Related commands

ipv6 access-list (named IPv6 hardware ACL)

ipv6 traffic-filter

match access-group

show ipv6 access-list (IPv6 Hardware ACLs)

show acl-group ipv6 address

Overview Use this command to show the hosts and subnets in a named IPv6 ACL group.

Syntax

```
show acl-group ipv6 address <group>
```

Parameter	Description
<group>	The name of the IPv6 ACL group.

Mode Privileged Exec

Example To show all hosts and subnets in an IPv6 ACL group IPV6_GROUP1, use the command:

```
awplus# show acl-group ipv6 address IPV6_GROUP1
```

Output Figure 40-1: Example output from **show acl-group ipv6 address IPV6_GROUP1**

```
awplus#show acl-group ipv6 address IPV6_GROUP1
Host Group: IPV6_GROUP1

 2001:DB8::/32
 2001:DB9::1/128
```

Related commands acl-group ipv6 address

ipv6 (ipv6-host-group)

Command changes Version 5.5.0-1.1: command added

show ipv6 access-list (IPv6 Hardware ACLs)

Overview Use this command to display all configured hardware IPv6 access-lists or the IPv6 access-list specified by name. Omitting the optional name parameter will display all IPv6 ACLs.

Syntax

```
show ipv6 access-list [<name>]
```

Parameter	Description
<name>	Hardware IPv6 access-list name.

Mode User Exec and Privileged Exec

Example To show all configured IPv6 access-lists use the command:

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

Output Figure 40-2: Example output from the **show ipv6 access-list** command

```
IPv6 access-list deny_ssh
  deny tcp abcd::0/64 any eq 22
```

Related commands

ipv6 access-list (named IPv6 hardware ACL)

(named IPv6 hardware ACL: ICMP entry)

(named IPv6 hardware ACL: IPv6 packet entry)

(named IPv6 hardware ACL: IP protocol entry)

(named IPv6 hardware ACL: TCP or UDP entry)

ipv6 traffic-filter

41 IPv6 Software Access Control List (ACL) Commands

Introduction

Overview This chapter provides an alphabetical reference for the IPv6 Software Access Control List (ACL) commands, and contains detailed command information and command examples about IPv6 software ACLs as applied to Routing and Multicasting, which are not applied to interfaces.

For information about ACLs, see the ACL Feature Overview and Configuration Guide.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see the following references:

- the Link Aggregation Feature Overview_and_Configuration_Guide.
- Link Aggregation Commands

Note that text in parenthesis in command names indicates usage not keyword entry. For example, **ipv6-access-list (named)** indicates named IPv6 ACLs entered as:

```
ipv6-access-list<name>
```

where <*name*> is a placeholder not a keyword.

Note also that parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI. For example, **(ipv6 access-list standard IPv6 filter)** represents command entry in the format shown in the syntax:

```
[<sequence-number>] {deny|permit}
{<source-ipv6-address/prefix-length>|any}
```

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Sub-modes Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 41-1: IPv6 Software Access List Commands and Prompts

Command Name	Command Mode	Prompt
show ipv6 access-list (IPv6 Software ACLs)	Privileged Exec	`awplus#`
ipv6 access-list extended (named)	Global Configuration	`awplus(config)#`
ipv6 access-list standard (named)	Global Configuration	`awplus(config)#`
(ipv6 access-list extended IP protocol filter)	IPv6 Extended ACL Configuration	`awplus(config-ipv6-ext-acl)#`
(ipv6 access-list extended TCP UDP filter)	IPv6 Extended ACL Configuration	`awplus(config-ipv6-ext-acl)#`
(ipv6 access-list standard filter)	IPv6 Standard ACL Configuration	`awplus(config-ipv6-std-acl)#`

Command List

- "ipv6 access-list extended (named)" on page 2043
- "ipv6 access-list extended proto" on page 2047
- "(ipv6 access-list extended IP protocol filter)" on page 2050
- "(ipv6 access-list extended TCP UDP filter)" on page 2053
- "ipv6 access-list standard (named)" on page 2055
- "(ipv6 access-list standard filter)" on page 2057
- "ipv6 prefix-list" on page 2059
- "show ipv6 access-list (IPv6 Software ACLs)" on page 2061
- "show ipv6 prefix-list" on page 2063
- "vty ipv6 access-class (named)" on page 2064

ipv6 access-list extended (named)

Overview

Use this command when configuring an IPv6 extended access-list for filtering frames that permit or deny IP, ICMP, TCP, UDP packets or ICMP packets with a specific value based on the source or destination.

The **no** variant of this command removes a specified IPv6 extended access-list.

Syntax [list-name]

```
ipv6 access-list extended <list-name>
no ipv6 access-list extended <list-name>
```

Parameter	Description
<list-name>	A user-defined name for the IPv6 software extended access-list.

Syntax [any|icmp|ip]

```
ipv6 access-list extended <list-name> {deny|permit}
{any|icmp|ip} {<ipv6-source-address/prefix-length>|any}
{<ipv6-destination-address/prefix-length>|any} [<icmp-type
<icmp-type>][log]
no ipv6 access-list extended <list-name> {deny|permit}
{any|icmp|ip} {<ipv6-source-address/prefix-length>|any}
{<ipv6-destination-address/prefix-length>|any} [<icmp-type
<icmp-type>][log]
```

Syntax [tcp|udp]

```
ipv6 access-list extended <list-name> {deny|permit} {tcp|udp}
{<ipv6-source-address/prefix-length>|any} {eq <sourceport>|lt
<sourceport>|gt <sourceport>|ne
<sourceport>}{<ipv6-destination-address/prefix-length>|any}
{eq <destport>|lt <destport>|gt <destport>|ne <destport>} [log]
no ipv6 access-list extended <list-name> {deny|permit}
{tcp|udp} {<ipv6-source-address/prefix-length>|any} {eq
<sourceport>|lt <sourceport>|gt <sourceport>|ne
<sourceport>}{<ipv6-destination-addr/prefix-length>|any} {eq
<destport>|lt <destport>|gt <destport>|ne <destport>} [log]
```

Parameter	Description
<list-name>	A user-defined name for the IPv6 software extended access-list.
deny	The IPv6 software extended access-list rejects packets that match the type, source, and destination filtering specified with this command.
permit	The IPv6 software extended access-list permits packets that match the type, source, and destination filtering specified with this command.

Parameter	Description
any	For ICMP|IP The IPv6 software extended access-list matches any type of packet.
ip	For ICMP|IP The IPv6 software extended access-list matches only IP packets.
icmp	For ICMP|IP The IPv6 software extended access-list matches only ICMP packets.
tcp	For TCP/UDP The IPv6 software extended access-list matches only TCP packets.
udp	For TCP/UDP The IPv6 software extended access-list matches only UDP packets.
<ipv6-source-address/prefix-length>	Specifies a source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<ipv6-destination-address/prefix-length>	Specifies a destination address and prefix length. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Matches any IPv6 address.
<sourceport>	For TCP/UDP The source port number, specified as an integer between 0 and 65535.
<destport>	For TCP/UDP The destination port number, specified as an integer between 0 and 65535.
icmp-type	For ICMP|IP Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets.
eq	For TCP/UDP Matches port numbers equal to the port number specified immediately after this parameter.
lt	For TCP/UDP Matches port numbers less than the port number specified immediately after this parameter.
gt	For TCP/UDP Matches port numbers greater than the port number specified immediately after this parameter.
ne	For TCP/UDP Matches port numbers not equal to the port number specified immediately after this parameter.

Parameter	Description	
<icmp-type>	For ICMP|IP The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type:	
	0	Echo replies.
	3	Destination unreachable messages.
	4	Source quench messages.
	5	Redirect (change route) messages.
	8	Echo requests.
	11	Time exceeded messages.
	12	Parameter problem messages.
	13	Timestamp requests.
	14	Timestamp replies.
	15	Information requests.
	16	Information replies.
	17	Address mask requests.
	18	Address mask replies.
`log`	Logs the results.	

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes Use IPv6 extended access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 extended access-list when a match is encountered.

For backwards compatibility you can either create IPv6 extended access-lists from within this command, or you can enter `ipv6 access-list extended` followed by only the IPv6 extended access-list name. This latter (and preferred) method moves you to the `(config-ipv6-ext-acl)` prompt for the selected IPv6 extended access-list number, and from here you can configure the filters for this selected access-list.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example 1 [creating a list]

To add a new filter to the access-list named `my-list` that will reject incoming ICMP packets from 2001:0db8::0/64 to 2001:0db8::f/64, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# icmp 2001:0db8::0/64
2001:0db8::f/64
```

Example 2 [adding to a list]

To insert a new filter at sequence number `5` of the access-list named `my-list`that will accept ICMP type 8 packets from the 2001:0db8::0/64 network to the 2001:0db8::f/64 network, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 icmp 2001:0db8::0/64
2001:0db8::f/64
```

Example 3 [list with filter]

To create the access-list named TK to deny TCP protocols, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended TK deny tcp any eq 14
any lt 12 log
```

Related commands

ipv6 access-list extended proto

(ipv6 access-list extended IP protocol filter)

(ipv6 access-list extended TCP UDP filter)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

Command changes

Version 5.5.1-0.1: Support for the **no** variant added

ipv6 access-list extended proto

Overview Use this command when configuring an IPv6 extended access-list for filtering frames that permit or deny packets with a specific value based on the IP protocol number specified.

The **no** variant of this command removes a specified IPv6 extended access-list with an IP protocol number.

Syntax

```
ipv6 access-list extended <list-name> {deny|permit} proto
<ip-protocol>} {<ipv6-source-address/prefix>|any}
{<ipv6-destination-address/prefix>|any} [log]
```

```
no ipv6 access-list extended <list-name> {deny|permit} proto
<ip-protocol>{<ipv6-source-address/prefix>|any}
{<ipv6-destination-address/prefix>|any} [log]
```

Parameter	Description
<list-name>	A user-defined name for the IPv6 software extended access- list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
proto	The IP Protocol type specified by its protocol number in the range 1 to 255.
<ip-protocol>	The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.
<ipv6-source-address/prefix>	IPv6 source address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any source address or local address.
<ipv6-destination-address/prefix>	IPv6 destination address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any destination address or remote address.
log	Log the results.

Table 41-2: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]

Table 41-2: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt

Table 41-2: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes Use IPv6 extended access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 extended access-list when a match is encountered.

The filter entry will match on any IP protocol type packet that has the specified source and destination IPv6 addresses and the specified IP protocol type. The parameter `any` may be specified if an address does not matter.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To create the IPv6 access-list named `ACL-1` to deny IP protocol `9` packets from `2001:0db8:1::1/128` to `2001:0db8:f::1/128`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended ACL-1 deny proto 9
2001:0db8:1::1/128 2001:0db8:f::1/128
```

To remove the IPv6 access-list named `ACL-1` to deny IP protocol `9` packets from `2001:0db8:1::1/128` to `2001:0db8:f::1/128`, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 access-list extended ACL-1 deny proto
10 2001:0db8:1::1/128 2001:0db8:f::1/128
```

Related commands

ipv6 access-list extended (named)

(ipv6 access-list extended IP protocol filter)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

(ipv6 access-list extended IP protocol filter)

Overview Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with or without an IP protocol specified, to the current extended IPv6 access-list. If a sequence is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with or without an IP protocol filter entry, from the current extended IPv6 access-list. You can specify the ACL filter entry by entering either its sequence number, or its filter entry profile.

Syntax [ip|proto]

```
[<sequence-number>] {deny|permit} {ip|any|proto <ip-protocol>}
{<ipv6-source-address/prefix>|any}
{<ipv6-destination-address/prefix>|any} [log]

no {deny|permit} {ip|any|proto <ip-protocol>}
{<ipv6-source-address/prefix>|any}
{<ipv6-destination-address/prefix>|any} [log]

no [<sequence-number>]
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
ip	IP packet.
any	Any packet.
proto *<ip-protocol>*	<1-255> Specify IP protocol number, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.
<ipv6-source-address/prefix>	IPv6 source address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any source address or local address.
<ipv6- destination-address/prefix>	IPv6 destination address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any destination address or remote address.
log	Log the results.

Table 41-3: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828

Table 41-3: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode IPv6 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes The filter entry will match on any IP protocol type packet that has the specified source and destination IPv6 addresses and the specified IP protocol type. The parameter `any` may be specified if an address does not matter.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To add a new ACL filter entry to the extended IPv6 access-list named `my-list` with sequence number `5` rejecting the IPv6 packet from `2001:db8:1:1` to `2001:db8:f:1`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 deny ip 2001:db8:1::1/128
2001:db8:f::1/128
```

To remove the ACL filter entry to the extended IPv6 access-list named `my-list` with sequence number `5`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# no 5
```

Related commands

ipv6 access-list extended (named)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

(ipv6 access-list extended TCP UDP filter)

Overview Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with a TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) source and destination port specified, to the current extended IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with a TCP or UDP source and destination port specified, from the current extended IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

Syntax [tcp|udp]

```
[<sequence-number>] {deny|permit} {tcp|udp}
{<ipv6-source-address/prefix>|any} {eq <sourceport>|lt
<sourceport>|gt <sourceport>|ne <sourceport>}
{<IPv6-destination-address/prefix>|any} {eq <destport>|lt
<destport>|gt <destport>|ne <destport>} [log]
```

```
no {deny|permit} {tcp|udp} {<ipv6-source-address/prefix>|any}
{eq <sourceport>|lt <sourceport>|gt <sourceport>|ne
<sourceport>}} {<IPv6-destination-address/prefix>|any} {eq
<destport>|lt <destport>|gt <destport>|ne <destport>} [log]
```

```
no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
tcp	TCP packet.
udp	UDP packet.
<ipv6-source-address/prefix>	IPv6 source address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any source address or local address.
eq	Equal to.
lt	Less than.
gt	Greater than.
ne	Not equal to.
<sourceport>	The source port number, specified as an integer between 0 and 65535.

Parameter	Description
<ipv6-destination-address/prefix>	IPv6 destination address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<destport>	The destination port number, specified as an integer between 0 and 65535.
`log`	Log the results.

Mode IPv6 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes The filter entry will match on any packet that has the specified source and destination IPv6 addresses and the specified TCP or UDP source and destination port. The parameter `any` may be specified if an address does not matter.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To add a new filter entry with sequence number `5` to the access-list named `my-list` to reject TCP packets from 2001:0db8::0/64 port `10` to 2001:0db8::f/64 port `20`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 deny tcp 2001:0db8::0/64 eq 10
2001:0db8::f/64 eq 20
```

To add a new filter entry with sequence number `5` to the extended IPv6 access-list named `my-list` to reject UDP packets from 2001:0db8::0/64 port `10` to 2001:0db8::f/ 64 port `20`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 deny udp 2001:0db8::0/64 eq 10
2001:0db8::f/64 eq 20
```

To remove the filter entry with sequence number `5`to the extended IPv6 access-list named `my-list`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# no 5
```

Related commands ipv6 access-list extended (named)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

ipv6 access-list standard (named)

Overview This command configures an IPv6 standard access-list for filtering frames that permit or deny IPv6 packets from a specific source IPv6 address.

The **no** variant of this command removes a specified IPv6 standard access-list.

Syntax [list-name]

```
ipv6 access-list standard <ipv6-acl-list-name>
no ipv6 access-list standard <ipv6-acl-list-name>
```

Parameter	Description
<ipv6-acl-list-name>	A user-defined name for the IPv6 software standard access-list.

Syntax [deny|permit]

```
ipv6 access-list standard <ipv6-acl-list-name> [{deny|permit}
{<ipv6-source-address/prefix-length>|any} [exact-match]]
no ipv6 access-list standard <ipv6-acl-list-name>
[{deny|permit} {<ipv6-source-address/prefix-length>|any}
[exact-match]]
```

Parameter	Description
<ipv6-acl-list-name>	A user-defined name for the IPv6 software standard access-list.
`deny`	The IPv6 software standard access-list rejects packets that match the type, source, and destination filtering specified with this command.
`permit`	The IPv6 software standard access-list permits packets that match the type, source, and destination filtering specified with this command.
<ipv6-source-address/ prefix-length>	Specifies a source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
`any`	Matches any source IPv6 address.
`exact-match`	Exact match of the prefixes.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage notes Use IPv6 standard access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 standard access-list when a match is encountered.

For backwards compatibility you can either create IPv6 standard access-lists from within this command, or you can enter `ipv6 access-list standard` followed by only the IPv6 standard access-list name. This latter (and preferred) method moves you to the `(config-ipv6-std-acl)` prompt for the selected IPv6 standard access-list, and from here you can configure the filters for this selected IPv6 standard access-list.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example To enter the IPv6 Standard ACL Configuration mode for the access-list named `my-list`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)#
```

Related commands

(ipv6 access-list standard filter)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

(ipv6 access-list standard filter)

Overview Use this ACL filter to add a filter entry for an IPv6 source address and prefix length to the current standard IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a filter entry for an IPv6 source address and prefix from the current standard IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

Syntax [icmp]

```
[<sequence-number>] {deny|permit}
{<ipv6-source-address/prefix-length>|any}
no {deny|permit} {<ipv6-source-address/prefix-length>|any}
no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
<ipv6-source-address/prefix-length>	IPv6 source address and prefix-length in the form X:X::X:X/P.
any	Any IPv6 source host address.

Mode IPv6 Standard ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage The filter entry will match on any IPv6 packet that has the specified IPv6 source address and prefix length. The parameter `any` may be specified if an address does not matter.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To add an ACL filter entry with sequence number `5` that will deny any IPv6 packets to the standard IPv6 access-list named `my-list`, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# 5 deny any
```

To remove the ACL filter entry that will deny any IPv6 packets from the standard IPv6 access-list named `my-list`, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# no deny any
```

Alternately, to remove the ACL filter entry with sequence number `5` to the standard IPv6 access-list named `my-list`, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# no 5
```

Related commands

ipv6 access-list standard (named)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

ipv6 prefix-list

Overview Use this command to create an IPv6 prefix list or an entry in an existing prefix list.

Use the **no** variant of this command to delete a whole prefix list, a prefix list entry, or a description.

Syntax

```
ipv6 prefix-list <list-name> [seq <1-429496725>] {deny|permit}
{any|<ipv6-prefix>} [ge <0-128>] [le <0-128>]
ipv6 prefix-list <list-name> description <text>
no ipv6 prefix-list <list-name> [seq <1-429496725>]
no ipv6 prefix-list <list-name> [description <text>]
```

Parameter	Description
`<list-name>`	Specifies the name of a prefix list.
`seq <1-429496725>`	Sequence number of the prefix list entry.
`deny`	Specifies that the prefixes are excluded from the list.
`permit`	Specifies that the prefixes are included in the list.
`<ipv6-prefix>`	Specifies the IPv6 prefix and prefix length in hexadecimal in the format X:X::X:X/M.
`any`	Any prefix match. Same as ::0/0 le 128.
`ge <0-128>`	Specifies the minimum prefix length to be matched.
`le <0-128>`	Specifies the maximum prefix length to be matched.
`description`	Prefix list specific description.
`<text>`	Up to 80 characters of text description of the prefix list.

Mode Global Configuration

Usage notes When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the **seq** parameter and place common permits or denials towards the top of the list. If you do not use the **seq** parameter, the sequence values are generated in a sequence of 5.

The parameters **ge** and **le** specify the range of the prefix lengths to be matched. The parameters **ge** and **le** are only used if an ip-prefix is stated. When setting these parameters, set the **le** value to be less than 128, and the **ge** value to be less than or equal to the **le** value and greater than the ip-prefix mask length.

Prefix lists implicitly exclude prefixes that are not explicitly permitted in the prefix list. This means if a prefix that is being checked against the prefix list reaches the end of the prefix list without matching a permit or deny, this prefix will be denied.

Example To check the first 32 bits of the prefix 2001:db8:: and that the subnet mask must be greater than or equal to 34 and less than or equal to 40, enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 prefix-list mylist seq 12345 permit
2001:db8::/32 ge 34 le 40
```

Related commands

match ipv6 address

show ipv6 prefix-list

show running-config ipv6 prefix-list

show ipv6 access-list (IPv6 Software ACLs)

Overview Use this command to display all configured IPv6 access-lists or the IPv6 access-list specified by name.

Syntax

```
show ipv6 access-list [<access-list-name>]
show ipv6 access-list standard [<access-list-name>]
show ipv6 access-list extended [<access-list-name>]
```

Parameter	Description
<access-list-name>	Only display information about an IPv6 access-list with the specified name.
`standard`	Only display information about standard access-lists.
`extended`	Only display information about extended access-lists.

Mode User Exec and Privileged Exec

Example To show all configured IPv6 access-lists, use the following command:

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

Output Figure 41-1: Example output from **show ipv6 access-list**

```
IPv6 access-list deny_icmp
  deny icmp any any vlan 1

IPv6 access-list deny_ssh
  deny tcp abcd::0/64 any eq 22
```

Example To show the IPv6 access-list named **deny_icmp,** use the following command:

```
awplus# show ipv6 access-list deny_icmp
```

Output Figure 41-2: Example output from **show ipv6 access-list** for a named ACL

```
IPv6 access-list deny_icmp
  deny icmp any any vlan 1
```

Related commands

ipv6 access-list extended (named)

(ipv6 access-list extended IP protocol filter)

ipv6 access-list standard (named)

(ipv6 access-list extended TCP UDP filter)

(ipv6 access-list standard filter)

show ipv6 prefix-list

Overview Use this command to display the prefix-list entries.

Note that this command is valid for RIPng and BGP4+ routing protocols only.

Syntax

```
show ipv6 prefix-list [<name>|detail|summary]
```

Parameter	Description
<name>	Specify the name of an individual IPv6 prefix list.
`detail`	Specify this parameter to show detailed output for all IPv6 prefix lists.
`summary`	Specify this parameter to show summary output for all IPv6 prefix lists.

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 prefix-list
awplus# show ipv6 prefix-list 10.10.0.98/8
awplus# show ipv6 prefix-list detail
```

Related commands ipv6 prefix-list

vty ipv6 access-class (named)

Overview For IPv6, use this command to set a standard named software access list to be the management ACL. This is then applied to all available VTY lines for controlling remote access by Telnet and SSH. This command allows or denies packets containing the IPv6 addresses included in the ACL to create a connection to your device.

ACLs that are attached using this command have an implicit 'deny-all' filter as the final entry in the ACL. A typical configuration is to permit a specific address, or range of addresses, and rely on the 'deny-all' filter to block all other access.

Use the **no** variant of this command to remove the access list.

Syntax

```
vty ipv6 access-class <access-name>
no vty ipv6 access-class [<access-name>]
```

Parameter	Description
<access-name>	Specify an IPv6 standard software access-list name

Mode Global Configuration

Examples To set the named standard access-list named **access-ctrl** to be the IPv6 management ACL, use the following commands:

```
awplus# configure terminal
awplus(config)# vty ipv6 access-class access-ctrl
```

To remove **access-ctrl** from the management ACL, use the following commands:

```
awplus# configure terminal
awplus(config)# no vty ipv6 access-class access-ctrl
```

Output Figure 41-3: Example output from the **show running-config** command

```
awplus#showrunning-config|grep access-class

vty ipv6 access-class access-ctrl
```

Related commands

show running-config

vty access-class (numbered)

42 QoS Commands

Introduction

Overview This chapter provides an alphabetical reference for Quality of Service commands.

QoS uses ACLs. For more information about ACLs, see the ACL Feature Overview and Configuration Guide.

Command List

- "class" on page 2067
- "class-map" on page 2068
- "clear mls qos interface policer-counters" on page 2069
- "default-action" on page 2070
- "description (QoS policy-map)" on page 2071
- "egress-rate-limit" on page 2072
- "egress-rate-limit overhead" on page 2074
- "match access-group" on page 2075
- "match cos" on page 2077
- "match dscp" on page 2078
- "match eth-format protocol" on page 2079
- "match inner-cos" on page 2082
- "match inner-vlan" on page 2083
- "match ip-precedence" on page 2084
- "match mac-type" on page 2085
- "match tcp-flags" on page 2086
- "match vlan" on page 2087
- "mls qos cos" on page 2088
- "mls qos enable" on page 2089

- "mls qos map cos-queue" on page 2090
- "mls qos map premark-dscp" on page 2091
- "no police" on page 2093
- "police single-rate action" on page 2094
- "police twin-rate action" on page 2096
- "policy-map" on page 2098
- "priority-queue" on page 2099
- "remark-map" on page 2100
- "remark new-cos" on page 2102
- "service-policy input" on page 2104
- "show class-map" on page 2105
- "show mls qos" on page 2106
- "show mls qos interface" on page 2107
- "show mls qos interface policer-counters" on page 2110
- "show mls qos interface queue-counters" on page 2111
- "show mls qos interface storm-status" on page 2112
- "show mls qos maps cos-queue" on page 2113
- "show mls qos maps premark-dscp" on page 2114
- "show platform classifier statistics utilization brief" on page 2115
- "show policy-map" on page 2117
- "storm-action" on page 2118
- "storm-downtime" on page 2119
- "storm-protection" on page 2120
- "storm-rate" on page 2121
- "storm-window" on page 2122
- "trust dscp" on page 2123
- "wrr-queue disable queues" on page 2124
- "wrr-queue egress-rate-limit queues" on page 2125
- "wrr-queue weight queues" on page 2126

class

Overview Use this command to associate an existing class-map to a policy or policy-map (traffic classification), and to enter Policy Map Class Configuration mode to configure the class- map.

Use the **no** variant of this command to delete an existing class-map.

If your class-map does not exist, you can create it by using the class-map command.

Syntax

```
class {<name>|default}
no class <name>
```

Parameter	Description
<name>	Name of the (already existing) class-map.
`default`	Specify the default class-map.

Mode Policy Map Configuration

Example The following example creates the policy-map `pmap1`(using the policy-map command), then associates this to an already existing class-map named `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)#
```

Related commands class-map

policy-map

class-map

Overview Use this command to create a class-map.

Use the **no** variant of this command to delete the named class-map.

Syntax

```
class-map <name>
no class-map <name>
```

Parameter	Description
<name>	Name of the class-map to be created.

Mode Global Configuration

Example This example creates a class-map called `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)#
```

clear mls qos interface policer-counters

Overview Resets an interface's policer counters to zero. You can either clear a specific class-map, or you can clear all class-maps by not specifying a class map.

Syntax

```
clear mls qos interface <port> policer-counters [class-map
<class-map>]
```

Parameter	Description
<port>	The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa3), or a dynamic (LACP) channel group (e.g. po4).
`class-map`	Select a class-map.
<class-map>	Class-map name.

Mode Privileged Exec

Example To reset the policy counters to zero for all class-maps for port1.0.4, use the command:

```
awplus# clear mls qos interface port1.0.4 policer-counters
```

Related commands show mls qos interface policer-counters

default-action

Overview Sets the action for the default class-map belonging to a particular policy-map. The action for a non-default class-map depends on the action of any ACL that is applied to the policy-map.

The default action can therefore be thought of as specifying the action that will be applied to any data that does not meet the criteria specified by the applied matching commands.

Use the **no** variant of this command to reset to the default action of 'permit'.

Syntax

```
default-action <action>
no default-action
```

Parameter		Description
<action>	`permit`	Packets to permit.
	`deny`	Packets to deny.
	`send-to-cpu`	Specify packets to send to the CPU.
	`copy-to-cpu`	Specify packets to copy to the CPU.
	`copy-to-mirror`	Specify packets to copy to the mirror port.
	`send-to-mirror`	Specify packets to send to the mirror port.
	`send-to-vlan-port vlan <vid> port <port-number>`	Send matching packets to the specified port, tagged with the specified VLAN. The specified port must belong to the specified VLAN.

Default The default is **permit**.

Mode Policy Map Configuration

Examples To set the action for the default class-map to deny, use the command:

```
awplus(config-pmap)# default-action deny
```

To set the action for the default class-map to copy-to-mirror for use with the mirror interface command, use the command:

```
awplus(config-pmap)# default-action copy-to-mirror
```

Related commands mirror interface

description (QoS policy-map)

Overview Adds a textual description of the policy-map. This can be up to 80 characters long.

Use the **no** variant of this command to remove the current description from the policy-map.

Syntax

```
description <line>
no description
```

Parameter	Description
<line>	Up to 80 character long line description.

Mode Policy Map Configuration

Example To add the description, VOIP traffic, use the command:

```
awplus(config-pmap)# description VOIP traffic
```

egress-rate-limit

Overview Use this command to limit the amount of traffic that can be transmitted per second from this port.

Use the **no** variant of this command to disable the limiting of traffic egressing on the interface.

Syntax

```
egress-rate-limit <rate-limit> max-burst-size <size>
no egress-rate-limit
```

Parameter	Description
<rate-limit>	Bandwidth <1-10000000 units per second> (usable units: k, m, g). The egress rate limit can be configured in multiples of 64kbps. If you configure a value that is not an exact multiple of 64kbps, then the value will be rounded up to the nearest higher exact multiple of 64kbps. The minimum is 64 Kb. The default unit is Kb (**k**), but Mb (**m**) or Gb (**g**) can also be specified. The command syntax is not case sensitive, so a value such as 20m or 20M will be interpreted as 20 megabits.
<size>	The maximum burst size in kilobytes (k), megabytes (m) or gigabytes (g). The minimum value for the max-burst-size is 64 kilobytes. Only certain values are valid; if you enter an invalid value, the max-burst size will be rounded to the nearest valid value. The default value is the number of bytes that would be transmitted in one full second of transmission at the rate limit. We recommend setting the maximum burst size to approximately the number of bytes that would be transmitted in one-third of a second of transmission at the rate limit. This means entering a value of approximately *<rate-limit>*/24.

Mode Interface Configuration

Usage notes Egress rate limiting uses a token bucket system. The rate limit represents how fast the bucket fills and the maximum burst size represents its maximum depth. The maximum burst size enables the switch to groom upstream traffic so that it meets the requirements of upstream devices. See the examples for more detail about the resulting behavior.

Examples To set a rate limit on port 1.0.1 of 5Mbps and burst size of 200KB, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# egress-rate-limit 5m max-burst-size 200k
```

When maximum burst size is 200KB, a burst of up to approximately 200KB can be sent at line rate (100 or 1000Mbps) if there are packets in the queues to send. If

traffic is still sitting in the queues once the 200KB burst has been sent, then that traffic will be only transmitted at 5Mbps, not at line rate. If the average egress traffic rate is over 5Mbps, then the queues will fill up over time. When the queues become full, the switch will drop packets and/or send pause frames to the traffic source. You can enable the switch to send pause frames by entering the command **flowcontrol**.

To disable egress rate limiting on a port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no egress-rate-limit
```

Related commands egress-rate-limit overhead

Command changes Version 5.4.6-2.1: **max-burst-size** parameter added

egress-rate-limit overhead

Overview Use this command to allow for the size of packet preamble and inter-packet gap (the "overhead") in egress queue rate limiting on switch ports.

Doing this keeps the rate limit at the same percentage of line rate for all packet sizes. Otherwise, the percentage of line rate changes with packet size, because of the size of the overhead relative to smaller packets. This means smaller packets take up a larger percentage of the line rate.

Use the **no** variant of this command to turn off the overhead allowance.

Syntax

```
egress-rate-limit overhead <bytes>
no egress-rate-limit overhead
```

Parameter	Description
<bytes>	The number of bytes to allow for overhead. For standard ethernet packets, use a value of 20 bytes (8 bytes of preamble and a inter-packet gap of 12 bytes).

Default No overhead allowance

Mode Interface Configuration

Example To configure an overhead allowance of 20 bytes (8 bytes of preamble and a inter-packet gap of 12 bytes) on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# egress-rate-limit overhead 20
```

To return port1.0.1 to the default of no overhead allowance, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no egress-rate-limit overhead
```

Related commands egress-rate-limit

Command changes Version 5.4.9-2.1: command added

match access-group

Overview Use this command to apply an ACL to a class-map or VLAN.

Use the **no** variant of this command to remove the match.

Syntax

```
match access-group {<hw-IP-ACL>|<hw-MAC-ACL>|<hw-named-ACL>}
no match access-group
{<hw-IP-ACL>|<hw-MAC-ACL>|<hw-named-ACL>}
```

Parameter	Description
<hw-IP-ACL>	Specify a hardware IP ACL number in the range <3000-3699>.
<hw-MAC-ACL>	Specify a hardware MAC ACL number in the range <4000-4699>.
<hw-named-ACL>	Specify a hardware named ACL (IP, IPv6 or MAC address entries).

Mode Class Map or VLAN Access-Map

Usage notes First create an access-list that applies the appropriate action to matching packets. Then use the **match access-group** command to apply this access-list as desired. Note that this command will apply the access-list matching only to *incoming* data packets.

Examples To configure a class-map named "cmap1", which matches traffic against access-list 3001, which allows IP traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 3001 permit ip any any
awplus(config)# class-map cmap1
awplus(config-cmap)# match access-group 3001
```

To configure a class-map named "cmap2", which matches traffic against access-list 4001, which allows MAC traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 permit any any
awplus(config)# class-map cmap2
awplus(config-cmap)# match access-group 4001
```

To configure a class-map named "cmap3", which matches traffic against access-list "hw_acl", which allows IP traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware hw_acl
awplus(config-ip-hw-acl)# permit ip any any
awplus(config)# class-map cmap3
awplus(config-cmap)# match access-group hw_acl
```

To apply ACL 3001 to VLAN 48, where the ACL drops IP traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 3001 deny ip any any
awplus(config)# vlan access-map deny_all
awplus(config-vlan-access-map)# match access-group 3001
awplus(config-vlan-access-map)# exit
awplus(config)# vlan filter deny_all vlan-list 48 input
```

Related commands

class-map

vlan access-map

Command changes

Version 5.4.6-2.1: support for VLAN access-maps added

match cos

Overview Use this command to define a COS to match against incoming packets.

Use the **no** variant of this command to remove CoS.

Syntax

```
match cos <0-7>
no match cos
```

Parameter	Description
<0-7>	Specify the CoS value.

Mode Class Map Configuration

Examples To set the class-map's CoS to 4, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match cos 4
```

To remove CoS from a class-map, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match cos
```

match dscp

Overview Use this command to define the DSCP to match against incoming packets.

Use the **no** variant of this command to remove a previously defined DSCP.

Syntax

```
match dscp <0-63>
no match dscp
```

Parameter	Description
<0-63>	Specify DSCP value (only one value can be specified).

Mode Class Map Configuration

Usage Use the **match dscp** command to define the match criterion after creating a class-map.

Examples To configure a class-map named `cmap1` with criterion that matches DSCP 56, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match dscp 56
```

To remove a previously defined DSCP from a class-map named cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match dscp
```

Related commands class-map

match eth-format protocol

Overview This command sets the Ethernet format and the protocol for a class-map to match on.

Select one Layer 2 format and one Layer 3 protocol when you issue this command.

Use the **no** variant of this command to remove the configured Ethernet format and protocol from a class-map.

Syntax

```
match eth-format <layer-two-format> protocol
<layer-three-protocol>
```

```
no match eth-format protocol
```

The following eth-formats and protocols are available (note that not all options are available on all AlliedWare Plus switch models):

Parameter	Description
<layer-two-formats>	
802dot2-tagged	802.2 Tagged Packets (enter the parameter name).
802dot2-untagged	802.2 Untagged Packets (enter the parameter name).
ethii-tagged	EthII Tagged Packets (enter the parameter name).
ethii-untagged	EthII Untagged Packets (enter the parameter name).
ethii-any	EthII Tagged or Untagged Packets (enter the parameter name).
netwareraw-tagged	Netware Raw Tagged Packets (enter the parameter name).
netwareraw-untagged	Netware Raw Untagged Packets (enter the parameter name).
snap-tagged	SNAP Tagged Packets (enter the parameter name).
snap-untagged	SNAP Untagged Packets (enter the parameter name).
<layer-three-protocols>	
<word>	A Valid Protocol Number in hexidecimal.
any	Note that the parameter "any" is only valid when used with the netwarerawtagged and netwarerawuntagged protocol options.
sna-path-control	Protocol Number 04 (enter the parameter name or its number).
proway-lan	Protocol Number 0E (enter the parameter name or its number).
eia-rs Protocol	Number 4E (enter the parameter name or its number).
proway Protocol	Number 8E (enter the parameter name or its number).

Parameter	Description
ipx-802dot2	Protocol Number E0 (enter the parameter name or its number).
netbeui	Protocol Number F0 (enter the parameter name or its number).
iso-clns-is	Protocol Number FE (enter the parameter name or its number).
xdot75-internet	Protocol Number 0801(enter the parameter name or its number).
nbs-internet	Protocol Number 0802 (enter the parameter name or its number).
ecma-internet	Protocol Number 0803 (enter the parameter name or its number).
chaosnet	Protocol Number 0804 (enter the parameter name or its number).
xdot25-level-3	Protocol Number 0805 (enter the parameter name or its number).
arp Protocol	Number 0806 (enter the parameter name or its number).
xns-compat	Protocol Number 0807 (enter the parameter name or its number).
banyan-systems	Protocol Number 0BAD (enter the parameter name or its number).
bbn-simnet	Protocol Number 5208 (enter the parameter name or its number).
dec-mop-dump-ld	Protocol Number 6001 (enter the parameter name or its number).
dec-mop-rem-cdons	Protocol Number 6002 (enter the parameter name or its number).
dec-decnet	Protocol Number 6003 (enter the parameter name or its number).
dec-lat	Protocol Number 6004 (enter the parameter name or its number).
dec-diagnostic	Protocol Number 6005 (enter the parameter name or its number).
dec-customer	Protocol Number 6006 (enter the parameter name or its number).
dec-lavc	Protocol Number 6007 (enter the parameter name or its number).
rarp	Protocol Number 8035 (enter the parameter name or its number).
dec-lanbridge	Protocol Number 8038 (enter the parameter name or its number).

Parameter	Description
dec-encryption	Protocol Number 803D (enter the parameter name or its number).
appletalk	Protocol Number 809B (enter the parameter name or its number).
ibm-sna	Protocol Number 80D5 (enter the parameter name or its number).
appletalk-aarp	Protocol Number 80F3 (enter the parameter name or its number).
snmp	Protocol Number 814CV.
ethertalk-2	Protocol Number 809B (enter the parameter name or its number).
ethertalk-2-aarp	Protocol Number 80F3 (enter the parameter name or its number).
ipx-snap	Protocol Number 8137 (enter the parameter name or its number).
ipx-802dot3	Protocol Number FFFF (enter the parameter name or its number).
ip	Protocol Number 0800 (enter the parameter name or its number).
ipx	Protocol Number 8137 (enter the parameter name or its number).
ipv6	Protocol Number 86DD (enter the parameter name or its number).

Mode Class Map Configuration

Examples To set the eth-format to ethii-tagged and the protocol to 0800 (IP) for class-map cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match eth-format ethii-tagged protocol
0800
awplus(config-cmap)# match eth-format ethii-tagged protocol ip
```

To remove the eth-format and the protocol from the class-map cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match eth-format protocol
```

match inner-cos

Overview Sets the Inner CoS for a class-map to match on.

Use the **no** variant of this command to remove CoS.

Syntax

```
match inner-cos <0-7>
no match inner-cos
```

Parameter	Description
<0-7>	Specify the Inner CoS value.

Mode Class Map Configuration

Examples To set the class-map's inner-cos to 4, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match inner-cos 4
```

To remove CoS from the class-map, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match inner-cos
```

match inner-vlan

Overview Use this command to define the inner VLAN ID as match criteria.

Use the **no** variant of this command to disable the VLAN ID used as match criteria.

Syntax

```
match inner-vlan <1-4094>
no match inner-vlan
```

Parameter	Description
<1-4094>	The VLAN number.

Mode Class Map Configuration

Usage notes This command is used in double-tagged networks to match on a VLAN ID belonging to the client network. For more information on VLAN double-tagged networks, see the VLAN_Feature Overview and Configuration Guide.

Examples To configure a class-map named `cmap1` to match traffic from inner VLAN 3, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match inner-vlan 3
```

To disable the configured VLAN ID as a match criteria for the class-map named `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match inner-vlan
```

match ip-precedence

Overview Use this command to identify IP precedence values as match criteria.

Use the **no** variant of this command to remove IP precedence values from a class-map.

Syntax

```
match ip-precedence <0-7>
no match ip-precedence
```

Parameter	Description
<0-7>	The precedence value to be matched.

Mode Class Map Configuration

Example To configure a class-map named `cmap1` to match all IPv4 packets with a precedence value of `5`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match ip-precedence 5
```

match mac-type

Overview Use this command to set the MAC type for a class-map to match on.

Use **no** variant of this command to remove the MAC type match entry.

Syntax

```
match mac-type {l2bcast|l2mcast|l2ucast}
no match mac-type
```

Parameter	Description
l2bcast	Layer 2 Broadcast traffic.
l2mcast	Layer 2 Multicast traffic.
l2ucast	Layer 2 Unicast traffic.

Mode Class Map Configuration

Examples To set the class-map's MAC type to Layer 2 multicast, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match mac-type l2mcast
```

To remove the class-map's MAC type entry, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match mac-type
```

match tcp-flags

Overview Sets one or more TCP flags (control bits) for a class-map to match on.

Use the **no** variant of this command to remove one or more TCP flags for a class-map to match on.

Syntax

```
match tcp-flags [ack] [fin] [psh] [rst] [syn] [urg]
no match tcp-flags [ack] [fin] [psh] [rst] [syn] [urg]
```

Parameter	Description
ack	Acknowledge.
fin	Finish.
psh	Push.
rst	Reset.
syn	Synchronize.
urg	Urgent.

Mode Class Map Configuration

Examples To set the class-map's TCP flags to **ack** and **syn**, use the commands:

```
awplus# configure terminal
awplus(config)# class-map
awplus(config-cmap)# match tcp-flags ack syn
```

To remove the TCP flags **ack** and **rst**, use the commands:

```
awplus# configure terminal
awplus(config)# class-map
awplus(config-cmap)# no match tcp-flags ack rst
```

match vlan

Overview Use this command to define the VLAN ID as match criteria.

Use the **no** variant of this command to disable the VLAN ID used as match criteria.

Syntax

```
match vlan <1-4094>
no match vlan
```

Parameter	Description
<1-4094>	The VLAN number.

Mode Class Map Configuration

Examples To configure a class-map named `cmap1` to include traffic from VLAN 3, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match vlan 3
```

To disable the configured VLAN ID as a match criteria for the class-map named `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match vlan
```

mls qos cos

Overview This command assigns a CoS (Class of Service) user-priority value to untagged frames entering a specified interface. By default, all untagged frames are assigned a CoS value of 0.

Use the **no** variant of this command to return the interface to the default CoS setting for untagged frames entering the interface.

Syntax

```
mls qos cos <0-7>
no mls qos cos
```

Parameter	Description
<0-7>	The Class of Service, user-priority value.

Default By default, all untagged frames are assigned a CoS value of 0. Note that for tagged frames, the default behavior is not to alter the CoS value.

Mode Interface Configuration

Example To assign a CoS user priority value of 2 to all untagged packets entering port1.0.1 to port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# mls qos cos 2
```

mls qos enable

Overview Use this command to enable QoS.

Use the **no** variant of this command to globally disable QoS and remove all QoS configuration. The **no** variant of this command removes all class-maps, policy-maps, and policers that have been created. Running the **no mls qos** command will therefore remove all pre-existing QoS configurations on the switch.

Mode Global Configuration

Syntax

```
mls qos enable
no mls qos
```

Example To enable QoS on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# mls qos enable
```

mls qos map cos-queue

Overview Use this command to set the default CoS to egress queue mapping. This is the default queue mapping for packets that do not get assigned an egress queue via any other QoS functionality.

Use the **no** variant of this command to reset the cos-queue map back to its default setting. The default mappings for this command are:

```
CoS Priority :      0 1 2 3 4 5 6 7
---------------------------------
CoS QUEUE:          2 0 1 3 4 5 6 7
```

Syntax

```
mls qos map cos-queue <cos-priority> to <queue-number>
no mls qos map cos-queue
```

Parameter	Description
<cos-priority>	CoS priority value. Can take a value between 0 and 7.
<queue-number>	Queue number. Can take a value between 0 and 7.

Mode Global Configuration

Examples To map CoS 2 to queue 0, use the command:

```
awplus# configure terminal
awplus(config)# mls qos map cos-queue 2 to 0
```

To set the cos-queue map back to its defaults, use the command:

```
awplus# configure terminal
awplus(config)# no mls qos map cos-queue
```

Related commands show mls qos interface

mls qos map premark-dscp

Overview This command configures the premark-dscp map. It is used when traffic is classified by a class-map that has trust dscp configured. Based on a lookup DSCP, the map determines new QoS settings for the traffic.

The **no** variant of this command resets the premark-dscp map to its defaults. If no DSCP is specified then all DSCP entries will be reset to their defaults.

Syntax

```
mls qos map premark-dscp <0-63> to
{[new-dscp <0-63>][new-cos <0-7>]
[new-bandwidth-class {green|yellow|red}]}
```

```
no mls qos map premark-dscp [<0-63>]
```

Parameter	Description
`premark-dscp <0-63>`	The DSCP value on ingress.
`new-dscp <0-63>`	The DSCP value that the packet will have on egress. If unspecified, this value will remain the DSCP ingress value.
`new-cos <0-7>`	The CoS value that the packet will have on egress. If unspecified, this value will retain its value on ingress.
`new-bandwidth-class`	Modify Egress Bandwidth-class. If unspecified, this value will be set to green.
`green`	Egress Bandwidth-class green (marked down Bandwidth-class).
`yellow`	Egress Bandwidth-class yellow (marked down Bandwidth-class).
`red`	Egress Bandwidth-class red (marked down Bandwidth-class).

Mode Global Configuration

Usage notes With the trust dscp command set, this command (**mls qos map premark-dscp**) enables you to remap the DSCP, CoS, output queue, or bandwidth class values.

However, note that you cannot simultaneously change the DSCP and CoS, because they use the same byte in the IP header.

Example To set the entry for DSCP `1` to use a new DSCP of `2`, use the command:

```
awplus# configure terminal
awplus(config)# mls qos map premark-dscp 1 to new-dscp 2
```

Example To set the entry for DSCP 1 to use a new CoS of 3, and a new bandwidth class of yellow, use the command:

```
awplus# configure terminal
awplus(config)# mls qos map premark-dscp 1 to new-cos 3
new-bandwidth-class yellow
```

Example To reset the entry for DSCP 1 use the command:

```
awplus# configure terminal
awplus(config)# no mls qos map premark-dscp 1
```

Related commands show mls qos maps premark-dscp

trust dscp

no police

Overview Use this command to disable any policer previously configured on the class-map.

Syntax

```
no police
```

Mode Policy Map Class Configuration

Usage notes This command disables any policer previously configured on the class-map.

Example To disable policing on a class-map, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# no police
```

Related commands

police single-rate action

police twin-rate action

police single-rate action

Overview Configures a single-rate policer for a class-map.

Syntax

```
police single-rate <cir> <cbs> <ebs> action
{drop-red|remark-transmit}
```

Parameter	Description	
<cir>	Specify the Committed Information Rate (CIR) (1-100000000 kbps).	
<cbs>	Specify the Committed Burst Size (CBS) (0-16777216 bytes).	
<ebs>	Specify a Excess Burst Size (EBS) (0-16777216 bytes).	
`action`	Specify the action if the rate is exceeded.	
	`drop-red`	Drop the red packets.
	`remark-transmit`	Modify the packets using the remark map, then transmit. You can configure the remark map using the remark-map command.

Mode Policy Map Class Configuration

Usage notes You can use a policer to meter the traffic classified by the class-map and assign it to one of three bandwidth classes.

The bandwidth classes are green (conforming), yellow (partially-conforming), and red (non-conforming). A single-rate policer is based on three values. These are the average rate, minimum burst and maximum burst.

Color	Definition
`green`	The traffic rate is less than the average rate and minimum burst.
`yellow`	The traffic rate is between the minimum burst and the maximum burst.
`red`	The traffic rate exceeds the average rate and the maximum burst.

Using an action of drop-red means that any packets classed as red are discarded.

NOTE: *This command will not take effect when applied to a class-map that attaches to a channel group whose ports span processor instances.*

Note that the remark-map does not only apply to red traffic. If a remark-map is configured on the same class-map as the policer, then the remark-map will apply to green- colored and yellow-colored traffic irrespective of the value configured on the **action** parameter of the policer. So, even if **action** is configured to **drop-red,** the remark-map will be applied to green and yellow traffic. So, the **action** parameter only applies to red- colored traffic. If **action** is set to **drop-red**, then red

traffic is dropped; if **action** is set to **remark-transmit**, then the red traffic has the action of the remark map applied to it, and is then transmitted.

Example To configure a single rate meter measuring traffic of 100 Mbps that drops a sustained burst of traffic over this rate, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# police single-rate 100000 1875000
1875000 action drop-red
```

Related commands

no police

police twin-rate action

remark-map

police twin-rate action

Overview Configures a twin-rate policer for a class-map.

Syntax

```
police twin-rate <cir> <pir> <cbs> <pbs> action
{drop-red|remark-transmit}
```

Parameter	Description	
<cir>	Specify the Committed Information Rate (CIR) (1-100000000 kbps).	
<pir>	Specify the Peak Information Rate (PIR) (1-100000000 kbps).	
<cbs>	Specify the Committed Burst Size (CBS) (0-16777216 bytes).	
<pbs>	Specify the Peak Burst Size (PBS) (0-16777216 bytes).	
action	Specify the action if rate is exceeded.	
	drop-red	Drop the red packets.
	remark-transmit	Modify the packets using the remark map, then transmit. You can configure the remark map using the remark-map command.

Mode Policy Map Class Configuration

Usage notes A policer can be used to meter the traffic classified by the class-map and as a result will be given one of three bandwidth classes. These are green (conforming), yellow (partially- conforming), and red (non-conforming).

A twin-rate policer is based on four values. These are the minimum rate (CIR), minimum burst size (CBS), maximum rate (PIR), and maximum burst size (PBS). The following table shows how these values define the bandwidth classes.

Bandwidth Class	Definition
green	The sum of the number of existing (buffered) bytes plus those arriving at the port per unit time results in a value that is less than that set for the CBS.
yellow	The sum of the number of existing (buffered) bytes plus those arriving at the port per unit time results in a value that is between those set for the CBS and the PBS.
red	The sum of the number of existing (buffered) bytes plus those arriving at the port per unit time results in a value that exceeds that set for the PBS.

Using an action of drop-red means that any packets classed as red will be discarded.

Using an action of remark-transmit means that the packet will be remarked with the values configured in the policed-dscp map. The index into this map is determined by the DSCP in the packet.

Note that the remark-map does not only apply to red traffic. If a remark-map is configured on the same class-map as the policer, then the remark-map will apply to green- colored and yellow-colored traffic irrespective of the value configured on the **action** parameter of the policer. So, even if **action** is configured to **drop-red,** the remark-map will be applied to green and yellow traffic. So, the **action** parameter only applies to red-colored traffic. If **action** is set to **drop-red**, then red traffic is dropped; if **action** is set to **remark-transmit**, then the red traffic has the action of the remark map applied to it, and is then transmitted.

Example To configure a twin rate meter measuring a minimum rate of 10 Mbps and a maximum rate of 20 Mbps, and drop red packets, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# police twin-rate 10000 20000 1875000
3750000 action drop-red
```

To configure a twin rate meter measuring a minimum rate of 10 Mbps and a maximum rate of 20 Mbps that uses the premark map to remark any non-conforming traffic, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# police twin-rate 10000 20000 1875000
3750000 action remark-transmit
```

Related commands

no police

police single-rate action

policy-map

Overview Use this command to create a policy-map and to enter Policy Map Configuration mode to configure the specified policy-map.

Use the **no** variant of this command to delete an existing policy-map.

Syntax

```
policy-map <name>
no policy-map <name>
```

Parameter	Description
<name>	Name of the policy-map.

Mode Global Configuration

Example To create a policy-map called pmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)#
```

Related commands class-map

priority-queue

Overview This command configures strict priority-based scheduling on the specified egress queues. You must specify at least one queue.

Syntax

```
priority-queue [0][1][2][3][4][5][6][7]
```

Parameter	Description
`[0][1]...[7]`	Specify the queues that will use strict priority scheduling. With strict priority scheduling, the switch will completely empty the highest numbered queue first, then start processing the next lowest numbered queue.

Mode Interface Configuration.

Usage notes By default, the queues on all ports are set for priority queuing. You can change the queue emptying sequence to weighted round robin, by using the wrr-queue weight queues command. You can then use the priority-queue command to reset the selected queues to priority queuing.

Note that the emptying sequence for priority queuing is always highest queue number to lowest queue number.

Example To apply priority-based scheduling to egress queues 1 and 2, use the commands:

```
awplus#configure terminal
awplus(config)#interface port1.0.1
awplus(config-if)#priority-queue 1 2
```

Related commands

show mls qos interface

show mls qos interface queue-counters

wrr-queue weight queues

remark-map

Overview Use this command to configure the remark map. If a re-mark map is applied to a class, and a policer is also applied to the same class, then:

- green and yellow traffic will all be acted upon by the remark-map, and
- red traffic will be either dropped or acted upon by the remark-map, depending on whether the policer **action** is set to **drop-red** or **remark-transmit**.

The **no** variant of this command resets the remark map to its defaults. Specifying the bandwidth class is optional. If no bandwidth class is specified, then all bandwidth classes are reset to their defaults.

Syntax

```
remark-map [bandwidth-class {green|yellow|red}] to {[new-dscp <0-63>] [new-bandwidth-class {green|yellow|red}]}
```

```
no remark-map [bandwidth-class {green|yellow|red}] to {[new-dscp <0-63>] [new-bandwidth-class {green|yellow|red}]}
```

Parameter	Description
`bandwidth-class`	Specify the bandwidth class of packets to remark.
`green`	Remark green packets.
`yellow`	Remark yellow packets.
`red`	Remark red packets.
`new-dscp`	Specify the new DSCP value.
<0-63>	The DSCP value.
`new-bandwidth-class`	Specify the new bandwidth class.
`green`	Remark the packet green.
`yellow`	Remark the packet yellow.
`red`	Remark the packet red.

Mode Policy Map Class Configuration

Examples To remark the policed green traffic to a new DSCP of 2 and a new bandwidth class of yellow, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# remark-map bandwidth-class green to new-dscp 2 new-bandwidth-class yellow
```

To remark the policed green traffic to a new DSCP of 2, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# remark-map bandwidth-class green to
new-dscp 2
```

To reset the DSCP for all bandwidth classes, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# no remark-map to new-dscp
```

Related commands

police single-rate action

police twin-rate action

remark new-cos

Overview This command enables you to configure and remark either or both of:

- the CoS flag in the data packet
- the input into the CoS to queue map, thus changing the destination egress queue.

Syntax

```
remark new-cos <0-7> [internal|external|both]
no remark new-cos [internal|external|both]
```

Parameter	Description
`<0-7>`	The new value for the CoS flag and/or the input into the CoS to queue map.
`external`	Remarks the CoS flag in the packet.
`internal`	Remarks the new-CoS input into the CoS to queue map.
`both`	Remarks (with the same value) both the CoS flag in the packet and the input to the CoS to queue map.

Mode Policy Map Class Configuration

Usage notes The default CoS to Queue mappings are shown in the following table:

CoS Value	0	1	2	3	4	5	6	7
Egress Queue No	2	0	1	3	4	5	6	7

The relationship between this command and the CoS to queue map is shown in the following figure.

Figure 42-1: Remarking and the CoS to Q map

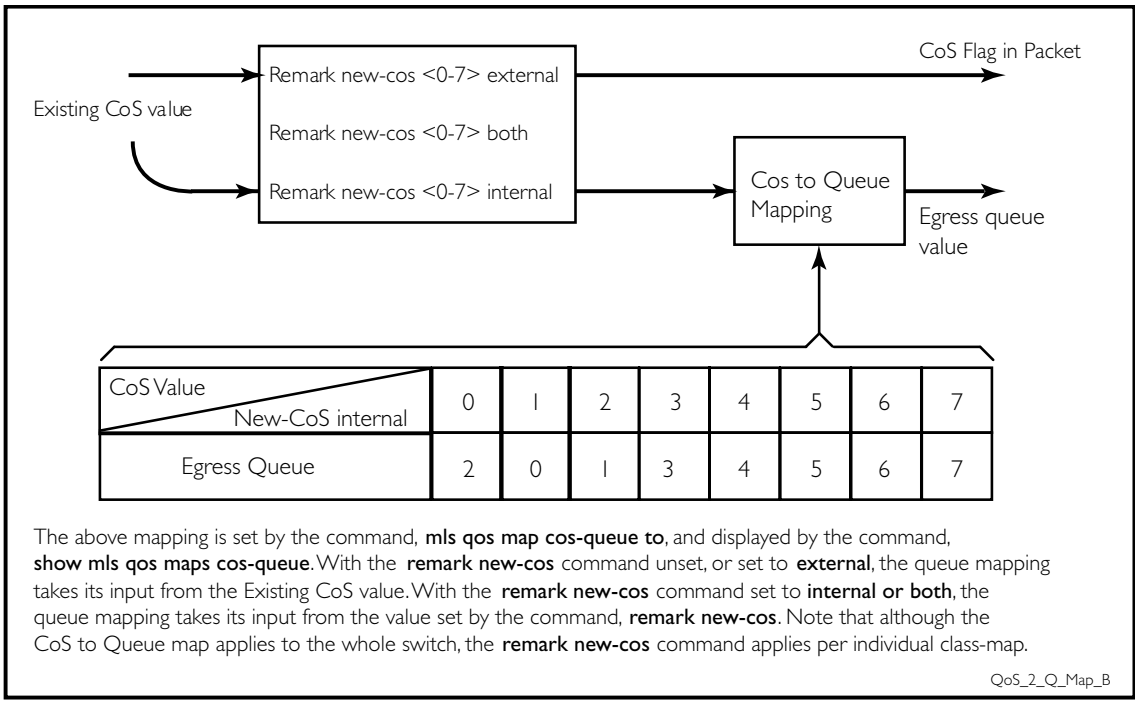


Table 42-1: CoS to egress queue remarking function

Input	Command	Output
CoS field = 1	Remark new-cos (not configured)	CoS value = 1 Packet sent to egress queue 0
CoS field = 1	Remark new-cos 2 external	CoS value = 2 Packet sent to egress queue 0
CoS set to 1	Remark new-cos 2 internal	CoS value = 1 Packet sent to egress queue 1
CoS set to 1	Remark new-cos 2 both	CoS value = 2 Packet sent to egress queue 1
Note: This table assumes that the CoS to Queue map is set to its default values.		

NOTE: *VLAN ID translation and VLAN double-tagging (switchport vlan translation) cannot be used on the same port in combination with CoS remarking.*

Example For policy-map "pmap3" and class-map "cmap1", set the CoS value to 2 and also set the input to the CoS to queue map so that the traffic is assigned to egress queue 1:

```
awplus# configure terminal
awplus(config)# policy-map pmap3
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# remark new-cos 2 both
```

Related commands

mls qos map cos-queue

show mls qos maps cos-queue

service-policy input

Overview Use this command to apply a policy-map to the input of an interface.

Use the **no** variant of this command to remove a policy-map and interface association.

Syntax

```
service-policy input <policy-map>
no service-policy input <policy-map>
```

Parameter	Description
<policy-map>	Policy map name that will be applied to the input.

Mode Interface Configuration

Usage notes This command can be applied to switch ports or static channel groups, but not to dynamic (LACP) channel groups.

Example To apply a policy-map named `pmap1` to interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
wplus(config-if)# service-policy input pmap1
```

show class-map

Overview Use this command to display the QoS class-maps' criteria for classifying traffic.

Syntax

```
show class-map [<class-map-name>]
```

Parameter	Description
<class-map-name>	Name of the class-map.

Mode User Exec and Privileged Exec

Example To display a QoS class-map's match criteria for classifying traffic, use the command:

```
awplus# show class-map cmap1
```

Output Figure 42-2: Example output from the **show class-map** command

```
awplus#show class-map

    CLASS-MAP-NAME: myClass
    Match Mac Type: 2 l2mcast

    CLASS-MAP-NAME: default
```

Related commands class-map

show mls qos

Overview Use this command to display whether QoS is enabled or disabled on the switch.

Syntax

```
show mls qos
```

Mode User Exec and Privileged Exec

Example To display whether QoS is enabled or disabled, use the command:

```
awplus# show mls qos
```

Output Figure 42-3: Example output from the **show mls qos** command

```
awplus#show mls qos
 Enable
```

Related commands mls qos enable

show mls qos interface

Overview Displays the current settings for the interface. This includes its default CoS and queue, scheduling used for each queue, and any policies/maps that are attached.

Syntax

```
show mls qos interface [<port>]
```

Parameter	Description
<port>	Switch port.

Mode User Exec and Privileged Exec

Example To display current CoS and queue settings for interface port1.0.1, use the command:

```
awplus# show mls qos interface port1.0.1
```

Output Figure 42-4: Example output from the **show mls qos interface** command for port1.0.1

```
awplus#show mls qos interface port1.0.1

Interface: port1.0.1

    Number of egress queues: 8

    Egress Queue:         0
      Status:             Enabled
      Scheduler:          Strict Priority
      Queue Limit:        12%
      Egress Rate Limit: 0 Kb

    Egress Queue:         1
      Status:             Enabled
      Scheduler:          Strict Priority
      Queue Limit:        12%
      Egress Rate Limit: 0 Kb
```

```
    Egress Queue:        2
      Status:            Enabled
      Scheduler:         Strict Priority
      Queue Limit:       12%
      Egress Rate Limit: 0 Kb
    Egress Queue:        3
      Status:            Enabled
      Scheduler:         Wrr Group 2
      Weight:            10
      Queue Limit:       12%
      Egress Rate Limit: 0 Kb
    Egress Queue:        4
      Status:            Enabled
      Scheduler:         Wrr Group 1
      Weight:            10
      Queue Limit:       12%
      Egress Rate Limit: 0 Kb
    Egress Queue:        5
      Status:            Enabled
      Scheduler:         Strict Priority
      Queue Limit:       12%
      Egress Rate Limit: 0 Kb
    Egress Queue:        6
      Status:            Enabled
      Scheduler:         Strict Priority
      Queue Limit:       12%
      Egress Rate Limit: 0 Kb
    Egress Queue:        7
      Status:            Enabled
      Scheduler:         Strict Priority
      Queue Limit:       12%
      Egress Rate Limit: 0 Kb
  Trust Mode: Ports default priority
  Port Default Priority: 0
  VLAN Priority Overide: Not Configured
  Egress Traffic Shaping Overhead: 20
  Egress Traffic Shaping: Not Configured
    The number of COS Values mapped: 8
    Cos (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 8(0), 9(0), 10(0), 11(0), 12(0), 13(0), 14(0), 15(0)
    Dscp (Queue): 16(0), 17(0), 18(0), 19(0), 20(0), 21(0), 22(0), 23(0)
    Dscp (Queue): 24(0), 25(0), 26(0), 27(0), 28(0), 29(0), 30(0), 31(0)
    Dscp (Queue): 32(0), 33(0), 34(0), 35(0), 36(0), 37(0), 38(0), 39(0)
    Dscp (Queue): 40(0), 41(0), 42(0), 43(0), 44(0), 45(0), 46(0), 47(0)
    Dscp (Queue): 48(0), 49(0), 50(0), 51(0), 52(0), 53(0), 54(0), 55(0)
    Dscp (Queue): 56(0), 57(0), 58(0), 59(0), 60(0), 61(0), 62(0), 63(0)
```

Table 42-2: Parameters in the output of the show mls qos interface command

Parameter	Description
`Number of egress queues`	The total number of egress queues available on this interface.
`Egress Queue`	Number of this egress queue.
`Status`	Queue can either be enabled or disabled.
`Scheduler`	The scheduling mode being used for servicing the transmission of packets on this port.
`Queue Limit`	The percentage of the port's buffers that have been allocated to this queue.
`Egress Rate Limit`	The amount of traffic that can be transmitted via this queue per second. 0 Kb means there is currently no rate-limiting enabled.
`Egress Traffic Shaping Overhead`	The number of bytes specified to allow for the size of packet preamble and inter-packet gap (the "overhead") in egress queue rate limiting. Use the egress-rate-limit overhead command to change this.

show mls qos interface policer-counters

Overview This command displays an interface's policer counters. This can either be for a specific class-map or for all class-maps attached to the interface. If no class-map is specified then all class-map policer counters attached to the interface are displayed.

Syntax

```
show mls qos interface <port> policer-counters [class-map
<class-map>]
```

Parameter	Description
<port>	Switch port.
`class-map`	Select a class-map.
<class-map>	Class-map name.

Mode User Exec and Privileged Exec

Usage Note that:

- The hardware does not record distinct counters for the number of Green or Yellow bytes, so the field marked Green/Yellow is the summation of bytes that have been marked Green or Yellow by the meter.
- The counters are based on metering performed on the specified class-map. Therefore, the 'Dropped Bytes' counter is the number of bytes dropped due to metering. This is different from packets dropped via a 'deny' action in the ACL. If a policer is configured to perform re-marking, bytes can be marked Red but are not dropped, and is shown with a value of 0 for the Dropped field and a non-0 value for the 'Red Bytes' field.

Example To show the counters for all class-maps attached to port1.0.1, use the command:

```
awplus# show mls qos interface port1.0.1 policer-counters
```

Output Figure 42-5: Example output from **show mls qos interface policer-counters** on a port

```
awplus#show mls qos interface port1.0.1 policer-counters
Interface:               port1.0.1
  Class-map:             default
    Green/Yellow Bytes:  0
    Red Bytes:           0
    Dropped Bytes:       0
    Non-dropped Bytes:   0
  Class-map:             cmap1
    Green/Yellow Bytes:  1290
    Red Bytes:           0
    Dropped Bytes:       0
    Non-dropped Bytes:   1290
```

show mls qos interface queue-counters

Overview This command displays an interface's egress queue counters. This can either be for a specific queue or for all queues on the interface. If no queue is specified all queue counters on the interface will be displayed.

The counters show the number of frames currently in the queue and the maximum number of frames allowed in the queue, for individual egress queues and the port's queue (which will be a sum of all egress queues).

Syntax

```
show mls qos interface <port> queue-counters [queue <number>]
```

Parameter	Description
<port>	Switch port.
queue *<number>*	Queue number, from 0 to 7.

Mode User Exec and Privileged Exec

Example To show the counters for all queues on port1.0.1, use the command:

```
awplus# show mls qos interface port1.0.1 queue-counters
```

Output Figure 42-6: Example output from **show mls qos interface queue-counters**

```
Interface port1.0.1 Queue Counters:
  Port queue length     1169
  Egress Queue length:
    Queue 0                0
    Queue 1                0
    Queue 2             1169
    Queue 3                0
    Queue 4                0
    Queue 5                0
    Queue 6                0
    Queue 7                0
```

Table 42-3: Parameters in the output from **show mls qos interface queue-counters**

Parameter	Description
Interface	Port we are showing the counters for.
Port queue length	Number of frames in the port's queue. This will be the sum of all egress queues on the port.
Egress Queue length	Number of frames in a specific egress queue.

show mls qos interface storm-status

Overview Show the current configuration and status of the QoS Storm Protection (QSP) on the given port.

Syntax

```
show mls qos interface <port> storm-status
```

Parameter	Description
<port>	Switch port.

Mode User Exec and Privileged Exec

Example To see the QSP status on port1.0.1, use the command:

```
awplus# show mls qos interface port1.0.1 storm-status
```

Output Figure 42-7: Example output from **show mls qos interface storm-status**

```
Interface:           port1.0.1
Storm-Protection:    Enabled
Port-status:         Enabled
Storm Action:        vlandisable
Storm Window:        5000 ms
Storm Downtime:      0 s
Timeout Remaining:   0 s
Last read data-rate: 0 kbps
Storm Rate:          1000 kbps
```

Related commands

storm-action

storm-downtime

storm-protection

storm-rate

storm-window

show mls qos maps cos-queue

Overview Show the current configuration of the cos-queue map.

Syntax

```
show mls qos maps cos-queue
```

Mode User Exec and Privileged Exec

Example To display the current configuration of the cos-queue map, use the command:

```
awplus# show mls qos maps cos-queue
```

Output Figure 42-8: Example output from **show mls qos maps cos-queue**

```
COS-TO-QUEUE-MAP:
      COS :                0 1 2 3 4 5 6 7
      ---------------------------------
      QUEUE:               2 0 1 3 4 5 6 7
```

Related commands mls qos map cos-queue

show mls qos maps premark-dscp

Overview This command displays the premark-dscp map. This map is used to replace the DSCP, CoS and/or bandwidth class of a packet matching the class-map, based on a lookup DSCP value.

Syntax

```
show mls qos maps premark-dscp [<0-63>]
```

Parameter	Description
<0-63>	DSCP table entry.

Mode User Exec and Privileged Exec

Example To display the premark-dscp map for DSCP 1, use the command:

```
awplus# show mls qos maps premark-dscp 1
```

Output Figure 42-9: Example output from the **show mls qos maps premark-dscp** command

```
PREMARK-DSCP-MAP:

    DSCP 1
    Bandwidth Class
    -------------------------
    New DSCP                2
    New CoS                 0
    New Bandwidth Class     green
```

Related commands mls qos map premark-dscp

trust dscp

show platform classifier statistics utilization brief

Overview This command displays the number of used entries available for various platform functions, and the percentage that number of entries represents of the total available.

Syntax
```
show platform classifier statistics utilization brief
```

Mode Privileged Exec

Example To display the platform classifier utilization statistics, use the following command:

```
awplus# show platform classifier statistics utilization brief
```

Output Figure 42-10: Output from **show platform classifier statistics utilization brief**

```
[Instance 0]
 Capacity:  503
  Number of Entries:
  Policy Type      Group ID   Used / Allocated
  ------------------------------------------------
  ACL              1476395010  119 /  119 (100%)
   Interface                  119
   VACL                         0
   AMFAPPS                      0
  DoS              Inactive      0 /    0 (  0%)
  VLAN Counter
   Group-Octet     Inactive      0 /    0 (  0%)
   Group-Packet    Inactive      0 /    0 (  0%)
  Flooding Nexthop Redirects Inactive      0 /    0 (  0%)
  Remote-Mirror    Inactive      0 /    0 (  0%)
  VLAN Isolate     Inactive      0 /    0 (  0%)
  QoS              Inactive      0 /    0 (  0%)

Rule Limit Reached (clear on read): 0
Total Rule Limit Reached from startup: 0
```

Output parameters Depending on your switch, you will see some of the following parameters in the output from **show platform classifier statistics utilization brief**

Parameter	Description
IPv6 Multicast	Reserved hardware space for use by IPv6 multicast, when the ipv6 multicast-routing command is used.
System	Fixed system entries. For example, resiliency links make use of system ACLs.
MLD Snooping	Entries to send various packets that MLD Snooping is interested in to the CPU.

Parameter	Description
DHCP Snooping	Entries used to send DHCP and ARP packets to the CPU. User-added DHCP Snooping filters under ACLs are counted under the ACL or QoS categories.
Loop Detection	Entries uses to send the special loop detection frame to the CPU.
EPSR	Entries used to send EPSR control traffic to the CPU.
CFM	Entries used by Connectivity Fault Management.
G8032	Entries used to send G.8032 control traffic to the CPU.
Global ACLs	Entries for ACLs appear here if the ACLs are applied globally instead of per switchport.
ACL	Entries for ACL filters that have been applied directly to ports using the access-group command.
VACL	Entries for VLAN-based ACLs (ACLs that are applied to VLANs instead of ports).
DOS	Entries used for Denial of Service protection.
UFO	Entries used by Upward Forwarding Only (UFO).
QoS	Entries for ACL filters and other class-map configurations, such as policers, applied through policy maps using the service input command.
RA Guard	Entries used to block IPv6 router advertisements, configured with the **ipv6 nd raguard** command.
AMFAPPS	Entries used by AMF Application Proxy. These entries enable the SES Controller to block infected ports.
Pre-Ingress	Entries used for VLAN ID Translation (and also for subnet-based and MAC-based VLAN entries on SBx81XLEM cards).
Egress	Entries used for VLAN ID Translation.
UDB	User Defined Bytes (UDB), which are a limited resource of bytes that can be used to implement additional arbitrary matching on packet bytes on some switches. The software manages the use and allocation of these bytes automatically. The output of this table is intended for use by Allied Telesis Customer Support only.

Related commands

show platform

ipv6 access-list (named IPv6 hardware ACL)

show policy-map

Overview Displays the policy-maps configured on the switch. The output also shows whether or not they are connected to a port (attached / detached) and shows their associated class-maps.

Syntax

```
show policy-map [<name>]
```

Parameter	Description
<name>	The name of a specific policy-map.

Mode User Exec and Privileged Exec

Example To display a listing of the policy-maps configured on the switch, use the command:

```
awplus# show policy-map
```

Output Figure 42-11: Example output from the **show policy-map** command

```
POLICY-MAP-NAME: example
  Interfaces:
  Default class-map action: permit

  CLASS-MAP-NAME: default
    Policer counters enabled
```

Related commands

no police

service-policy input

storm-action

Overview Sets the action to be taken when triggered by QoS Storm Protection (QSP). There are three available options:

- **portdisable** will disable the port in software.
- **vlandisable** will disable the port from the VLAN matched by the class-map in class-map. This option requires the match vlan class-map to be present in the class-map
- **linkdown** will physically bring the port down. .

The **no** variant of this command will negate the action set by the **storm-action** command.

Syntax

```
storm-action {portdisable|vlandisable|linkdown}
no storm-action
```

Parameter	Description
`portdisable`	Disable the port in software.
`vlandisable`	Disable the VLAN.
`linkdown`	Shutdown the port physically.

Mode Policy Map Class Configuration

Examples To apply the storm protection of **vlandisable** to the policy-map named “pmap2” and the class-map named “cmap1”, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c# storm-action vlandisable
```

To negate the storm protection set on the policy-map named “pmap2” and the class-map named “cmap1”, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c# no storm-action
```

Related commands

storm-downtime

storm-protection

storm-rate

storm-window

storm-downtime

Overview Sets the time to re-enable a port that has been disabled by QoS Storm Protection (QSP). The time is given in seconds, from a minimum of one second to maximum of 86400 seconds (i.e. one day).

The **no** variant of this command resets the time to the default value of 10 seconds.

Syntax

```
storm-downtime <1-86400>
no storm-downtime
```

Parameter	Description
<1-86400>	Seconds.

Default 10 seconds

Mode Policy Map Class Configuration

Examples To re-enable the port in 1 minute, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# storm-downtime 60
```

To re-set the port to the default (10 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# no storm-downtime
```

Related commands

storm-action

storm-protection

storm-rate

storm-window

storm-protection

Overview Use this command to enable policy-based Storm Protection (such as QSP - QoS Storm Protection). Storm protection is activated as soon as a port is enabled. However, it will only be functional after storm-rate and storm-window have been set.

The **no** variant of this command disables policy-based Storm Protection.

Syntax

```
storm-protection
no storm-protection
```

Default By default, storm protection is disabled.

Mode Policy Map Class Configuration

Examples To enable QSP on cmap2 in pmap2, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# storm-protection
```

To disable QSP on cmap2 in pmap2, use the following commands:

```
awplus# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# no storm-protection
```

Related commands

show mls qos interface storm-status

storm-action

storm-downtime

storm-rate

storm-window

storm-rate

Overview Sets the data rate that triggers the storm-action. The rate is in kbps and the range is from 1kbps to 40Gbps.

Note that this setting is made in conjunction with the storm-window command.

Use the **no** variant of this command to negate the **storm-rate** command.

Syntax

```
storm-rate <1-40000000>
no storm-rate
```

Parameter	Description
<1-40000000>	The range of the storm-rate.

Default No default

Mode Policy Map Class Configuration

Usage This setting is made in conjunction with the storm-window command.

Examples To limit the data rate to 100Mbps, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# storm-rate 100000
```

To negate the limit set previously, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# no storm-rate
```

Related commands

storm-action

storm-downtime

storm-protection

storm-window

storm-window

Overview Sets the window size of QoS Storm Protection (QSP). This sets the time to poll the data-rate every given milliseconds. Minimum window size is 100 ms and the maximum size is 60 sec.

Use the **no** variant of this command to negate the **storm-window** command.

Syntax

```
storm-window <100-60000>
no storm-window
```

Parameter	Description
<100-60000>	The window size, measured in milliseconds.

Default No default

Mode Policy Map Class Configuration

Usage This command should be set in conjunction with the storm-rate command.

Examples To set the QSP window size to `5000` ms, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# storm-window 5000
```

To negate the QSP window size set previously, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# no storm-window
```

Related commands

storm-action

storm-downtime

storm-protection

storm-rate

trust dscp

Overview This command enables the premark-dscp map to replace the DSCP, bandwidth-class and/or CoS of classified traffic based on a lookup DSCP value.

With the **no** variant of this command, no premark-dscp mapping function will be applied for the selected class-map. QoS components of the packet existing either at ingress, or applied by the class-map, will pass unchanged.

Syntax

```
trust dscp
no trust
```

Mode Policy-Map Configuration

Examples To enable the premark-dscp map lookup for policy-map pmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# trust dscp
```

To disable the premark-dscp map lookup for policy-map pmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# no trust
```

Related commands mls qos map premark-dscp

wrr-queue disable queues

Overview Use this command to disable an egress queue from transmitting traffic.

The **no** variant of this command enables an egress queue to transmit traffic.

Syntax

```
wrr-queue disable queues [0][1][2][3][4][5][6][7]
no wrr-queue disable queues [0][1][2][3][4][5][6][7]
```

Parameter	Description
`[0][2]...[7]`	Selects one or more queues numbered 0 to 7.

Mode Interface Configuration

Examples To disable queue 1 on port1.0.1 from transmitting traffic, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# wrr-queue disable queues 1
```

To enable queue 1 on port1.0.1 to transmit traffic, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no wrr-queue disable queues 1
```

Related commands show mls qos interface

wrr-queue egress-rate-limit queues

Overview Sets a limit on the amount of traffic that can be transmitted per second from these queues. The default unit is in Kb, but Mb or Gb can also be specified. The minimum is 651 Kb.

Syntax

```
wrr-queue egress-rate-limit <bandwidth> queues
[0][1][2][3][4][5][6][7]
```

```
no wrr-queue egress-rate-limit <bandwidth> queues
[0][1][2][3][4][5][6][7]
```

Parameter	Description
<bandwidth>	Bandwidth <1-100000000 kbits> (usable units: k, m, g).
[0][2]...[7]	Selects one or more queues numbered 0 to 7.

Mode Interface Configuration

Example To limit the egress rate of queues 0, 1 and 2 on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# wrr-queue egress-rate-limit 500M queues 0 1
2
```

Related commands show mls qos interface

wrr-queue weight queues

Overview This command configures weighted round-robin based scheduling on the specified egress queues on switch port interfaces only. The weights are specified as ratios relative to each other.

Use the **no wrr-queue** command to remove weighted round-robin based scheduling from the specified egress queue. The queue then reverts to its normal priority-based scheduling.

Syntax

```
wrr-queue weight <1-15> queues [0][1][2][3][4][5][6][7]
no wrr-queue <queue-number>
```

Parameter	Description
<1-15>	Weight (the higher the number the greater will be the queue servicing).
`[0][2]...[7]`	Selects one or more queues numbered 0 to 7.
<queue-number>	Egress queue to revert to priority-based scheduling.

Mode Interface Configuration for switch port interfaces only (not for static aggregated interfaces).

Usage notes You cannot apply weighted round-robin based scheduling to static aggregated interfaces (for example, sa2).

Example To apply a WRR weight of 6 to queues 0 and 1 on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# wrr-queue weight 6 queues 0 1
```

To remove weighted round-robin scheduling from egress queue 2 on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no wrr-queue 2
```

Related commands priority-queue

show mls qos interface

43 802.1X Commands

Introduction

Overview

802.1X is an IEEE standard providing a mechanism for authenticating devices attached to a LAN port or wireless device. Devices wishing to access services behind a port must authenticate themselves before any Ethernet packets are allowed to pass through. The protocol is referred to as 802.1X because it was initially defined in the IEEE standard 802.1X, published in 2001 and revised in 2004 and again as the current 802.1X 2010 standard.

This chapter provides an alphabetical reference of commands used to configure 802.1X port access control. For more information, see the AAA and Port Authentication_Feature Overview and Configuration Guide.

Command List

- "dot1x accounting" on page 2129
- "dot1x authentication" on page 2130
- "debug dot1x" on page 2131
- "dot1x control-direction" on page 2132
- "dot1x eap" on page 2134
- "dot1x eapol-version" on page 2135
- "dot1x initialize interface" on page 2136
- "dot1x initialize supplicant" on page 2137
- "dot1x keytransmit" on page 2138
- "dot1x max-auth-fail" on page 2139
- "dot1x max-reauth-req" on page 2141
- "dot1x port-control" on page 2143
- "dot1x timeout tx-period" on page 2145
- "show debugging dot1x" on page 2147
- "show dot1x" on page 2148

- "show dot1x diagnostics" on page 2151
- "show dot1x interface" on page 2153
- "show dot1x sessionstatistics" on page 2155
- "show dot1x statistics interface" on page 2156
- "show dot1x supplicant" on page 2157
- "show dot1x supplicant interface" on page 2159
- "undebug dot1x" on page 2161

dot1x accounting

Overview This command overrides the **default** RADIUS accounting method for IEEE 802.1X-based authentication on an interface by allowing you to apply a user-defined named method list.

Use the **no** variant of this command to remove the named list from the interface and apply the **default** method list.

Syntax

```
dot1x accounting {default|<list-name>}
no dot1x accounting
```

Parameter	Description
`default`	Apply the default accounting method list
<list-name>	Apply the user-defined named list

Default The **default** method list is applied to an interface by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To apply the named list 'vlan10_acct' on the vlan10 interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# dot1x accounting vlan10_acct
```

To remove the named list from the vlan10 interface and set the authentication method back to **default**, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no dot1x accounting
```

Related commands aaa accounting dot1x

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

dot1x authentication

Overview This command overrides the **default** 802.1X-based authentication method on an interface by allowing you to apply a user-defined named list.

Use the **no** variant of this command to remove the named list from the interface and apply the **default** method.

Syntax

```
dot1x authentication {default|<list-name>}
no dot1x authentication
```

Parameter	Description
default	Apply the default authentication method list
<list-name>	Apply the user-defined named list

Default The **default** method list is applied to an interface by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To apply the named list 'vlan10_auth' on the vlan10 interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# dot1x authentication vlan10_auth
```

To remove the named list from the vlan10 interface and set the authentication method back to **default**, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no dot1x authentication
```

Related commands aaa authentication dot1x

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

debug dot1x

Overview Use this command to enable 802.1X IEEE Port-Based Network Access Control troubleshooting functions.

Use the **no** variant of this command to disable this function.

Syntax

```
debug dot1x [all|auth-web|event|nsm|packet|timer]
no debug all dot1x
no debug dot1x [all|auth-web|event|nsm|packet|timer]
```

Parameter	Description
`all`	Used with the **no** variant of this command exclusively; turns off all debugging for 802.1X.
`auth-web`	Specifies debugging for 802.1X auth-web information.
`events`	Specifies debugging for 802.1X events.
`nsm`	Specifies debugging for NSM messages.
`packet`	Specifies debugging for 802.1X packets.
`timer`	Specifies debugging for 802.1X timers.

Mode Privileged Exec and Global Configuration

Usage notes This command turns on a mode where trace-level information is output during authentication conversations. Be aware that this is a very verbose output. It is mostly useful to capture this as part of escalating an issue to ATI support.

Examples Use this command without any parameters to turn on normal 802.1X debug information.

```
awplus# debug dot1x
awplus# show debugging dot1x
```

```
802.1X debugging status:
  802.1X events debugging is
  802.1X timer debugging is on
  802.1X packets debugging is on
  802.1X NSM debugging is on
```

Related commands show debugging dot1x

undebug dot1x

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

dot1x control-direction

Overview This command sets the direction of the filter for the unauthorized interface.

If the optional **in** parameter is specified with this command then packets entering the specified port are discarded. The **in** parameter discards the ingress packets received from the supplicant.

If the optional **both** parameter is specified with this command then packets entering (ingress) and leaving (egress) the specified port are discarded. The **both** parameter discards the packets received from the supplicant and sent to the supplicant.

The **no** variant of this command sets the direction of the filter to **both**. The port will then discard both ingress and egress traffic.

Syntax

```
dot1x control-direction {in|both}
no dot1x control-direction
```

Parameter	Description
`in`	Discard received packets from the supplicant (ingress packets).
`both`	Discard received packets from the supplicant (ingress packets) and transmitted packets to the supplicant (egress packets).

Default The authentication port direction is set to **both** by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the port direction to the default (**both**) for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x control-direction
```

To set the port direction to **in** for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x control-direction in
```

To set the port direction to **in** for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x control-direction in
```

Related commands

auth profile (global)

show dot1x

show dot1x interface

show auth interface

Command changes

Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

dot1x eap

Overview This command selects the transmit mode for the EAP packet. If the authentication feature is not enabled then EAP transmit mode is not enabled. The default setting discards EAP packets.

Syntax

```
dot1x eap {discard|forward|forward-untagged-vlan|forward-vlan}
```

Parameter	Description
`discard`	Discard.
`forward`	Forward to all ports on the switch.
`forward-untagged-vlan`	Forward to ports with the same untagged VLAN.
`forward-vlan`	Forward to ports with the same VLAN.

Default The transmit mode is set to `discard` EAP packets by default.

Mode Global Configuration

Examples To set the transmit mode of EAP packet to **forward**, to forward EAP packets to all ports on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward
```

To set the transmit mode of EAP packet to **discard**, to discard EAP packets, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap discard
```

To set the transmit mode of EAP packet to **forward-untagged-vlan**, to forward EAP packets to ports with the same untagged VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward-untagged-vlan
```

To set the transmit mode of EAP packet to **forward-vlan**, to forward EAP packets to ports with the same VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward-vlan
```

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

dot1x eapol-version

Overview This command sets the EAPOL protocol version for EAP packets when 802.1X port authentication is applied.

Use the **no** variant of this command to set the EAPOL protocol version to 1.

The default EAPOL protocol version is version 1.

Syntax

```
dot1x eapol-version {1|2}
no dot1x eapol-version
```

Parameter	Description
1|2	EAPOL protocol version 1 or 2.

Default The EAP version for 802.1X authentication is set to 1 by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the EAPOL protocol version to 2 for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x eapol-version 2
```

To set the EAPOL protocol version to the default version (1) for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x eapol-version
```

To set the EAPOL protocol version to 2 for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x eapol-version 2
```

Validation Commands auth profile (global)

show dot1x

show dot1x interface

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

dot1x initialize interface

Overview This command removes authorization for a specified connected interface. The connection will attempt to re-authorize when the specified port attempts to make use of the network connection.

NOTE: *Reauthentication could be a long time after the use of this command because the reauthorization attempt is not triggered by this command. The attempt is triggered by the first packet from the interface trying to access the network resources.*

Syntax

```
dot1x initialize interface <interface-list>
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • a continuous range of interfaces separated by a hyphen (e.g. port1.0.1-port1.0.3) • a comma-separated list (e.g. port1.0.1, port1.0.3-port1.0.4). Do not mix interface types in a list. The specified interfaces must exist.

Mode Privileged Exec

Examples To initialize 802.1X port authentication on the interface port1.0.2, use the command:

```
awplus# dot1x initialize interface port1.0.2
```

To unauthorize switch port1.0.2 and attempt reauthentication on switch port1.0.2, use the command:

```
awplus# dot1x initialize interface port1.0.2
```

To unauthorize all switch ports for a 18-port device and attempt reauthentication, use the command:

```
awplus# dot1x initialize interface port1.0.1-port1.0.18
```

Related commands

dot1x initialize supplicant

show dot1x

show dot1x interface

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

dot1x initialize supplicant

Overview This command removes authorization for a connected supplicant with the specified MAC address or username. The connection will attempt to re-authorize when the specified supplicant attempts to make use of the network connection.

NOTE: *Reauthentication could be a long time after the use of this command because the reauthorization attempt is not triggered by this command. The attempt is triggered by the first packet from the supplicant trying to access the network resources.*

Syntax

```
dot1x initialize supplicant {<macadd>|username}
```

Parameter	Description
`dot1x`	IEEE 802.1X Port-Based Access Control.
`initialize`	Initialize the port to attempt reauthentication.
`supplicant`	Specify the supplicant to initialize.
<macadd>	MAC (hardware address of the supplicant.
`username`	The name of the supplicant entry.

Mode Privileged Exec

Example To initialize the supplicant authentication, use the commands

```
awplus# configure terminal
awplus(config)# dot1x initialize supplicant 0090.99ab.a020
awplus(config)# dot1x initialize supplicant guest
```

Related commands

dot1x initialize interface

show dot1x

show dot1x supplicant

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

dot1x keytransmit

Overview Use this command to enable key transmission on the interface specified previously in Interface mode.

This command enables key transmission over an Extensible Authentication Protocol (EAP) packet between the authenticator and supplicant.

The **no** variant of this command disables key transmission on the interface specified.

Syntax

```
dot1x keytransmit
no dot1x keytransmit
```

Default Key transmission for port authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To enable the key transmit feature on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x keytransmit
```

To disable the key transmit feature on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x keytransmit
```

Related commands show dot1x

show dot1x interface

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

dot1x max-auth-fail

Overview Use this command to configure the maximum number of login attempts for a supplicant (client device) using the **auth-fail vlan** feature, when using 802.1X port authentication on an interface.

The **no** variant of this command resets the maximum login attempts for a supplicant (client device) using the auth-fail vlan feature, to the default configuration of 3 login attempts.

Syntax

```
dot1x max-auth-fail <0-10>
no dot1x max-auth-fail
```

Parameter	Description
<0-10>	Specify the maximum number of login attempts for supplicants on an interface using 802.1X port authentication.

Default The default maximum number of login attempts for a supplicant on an interface using 802.1X port authentication is 3 login attempts.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes This command sets the maximum number of login attempts for supplicants on an interface. The supplicant is moved to the auth-fail VLAN from the Guest VLAN after the number of failed login attempts using 802.1X authentication is equal to the number set with this command.

See the AAA and Port Authentication Feature Overview and Configuration Guide for information about:

- the auth-fail VLAN feature, and
- restrictions regarding combinations of authentication enhancements working together

Examples To configure the maximum number of login attempts for a supplicant on interface port1.0.2 to a single login attempt, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x max-auth-fail 1
```

To configure the maximum number of login attempts for a supplicant on interface port1.0.2 to the default number of 3 login attempts, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x max-auth-fail
```

To configure the maximum number of login attempts for a supplicant on authentication profile 'student' to a single login attempt, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x max-auth-fail 1
```

Related commands

auth auth-fail vlan

auth profile (global)

dot1x max-reauth-req

show dot1x interface

Command changes

Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

dot1x max-reauth-req

Overview Use this command to set the number of reauthentication attempts before an interface is unauthorized.

The **no** variant of this command resets the reauthentication delay to the default.

Syntax

```
dot1x max-reauth-req <1-10>
no dot1x max-reauth-req
```

Parameter	Description
<1-10>	Specify the maximum number of reauthentication attempts for supplicants on an interface using 802.1X port authentication.

Default The default maximum reauthentication attempts for interfaces using 802.1X port authentication is two (2) reauthentication attempts, before an interface is unauthorized.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes Use this command to set the maximum reauthentication attempts after failure.

Examples To configure the maximum number of reauthentication attempts for interface port1.0.2 to a single (1) reauthentication request, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x max-reauth-req 1
```

To configure the maximum number of reauthentication attempts for interface port1.0.2 to the default maximum number of two (2) reauthentication attempts, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x max-reauth-req
```

To configure the maximum number of reauthentication attempts for authentication profile 'student' to a single (1) reauthentication request, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x max-reauth-req 1
```

Related commands

auth profile (global)

dot1x max-auth-fail

show dot1x interface

Command changes

Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

dot1x port-control

Overview This command enables 802.1X port authentication on the interface specified, and sets the control of the authentication port.

The **no** variant of this command disables the port authentication on the interface specified.

Syntax

```
dot1x port-control {force-unauthorized|force-authorized|auto}
no dot1x port-control
```

Parameter	Description
`force-unauthorized`	Force the port state to unauthorized. Specify this to force a port to always be in an unauthorized state.
`force-authorized`	Force the port state to authorized. Specify this to force a port to always be in an authorized state.
`auto`	Allow the port client to negotiate authentication. Specify this to enable authentication on the port.

Default 802.1X port control is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes Use this command to force a port state.

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.

Examples To enable port authentication on the interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
```

To enable port authentication force authorized on the interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control force-authorized
```

To disable port authentication on the interface port1.0.2 use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x port-control
```

To enable port authentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x port-control auto
```

Related commands

aaa authentication dot1x

auth profile (global)

show dot1x interface

Command changes

Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

dot1x timeout tx-period

Overview This command sets the transmit timeout for the authentication request on the specified interface.

The **no** variant of this command resets the transmit timeout period to the default (30 seconds).

Syntax

```
dot1x timeout tx-period <1-65535>
no dot1x timeout tx-period
```

Parameter	Description
<1-65535>	Seconds.

Default The default transmit period for port authentication is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes Use this command to set the interval between successive attempts to request an ID.

Examples To set the transmit timeout period to 5 seconds on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x timeout tx-period 5
```

To reset transmit timeout period to the default (30 seconds) on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x timeout tx-period
```

To set the transmit timeout period to 5 seconds on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x timeout tx-period 5
```

Related commands

auth profile (global)

show dot1x

show dot1x interface

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

show debugging dot1x

Overview Use this command to see what debugging is turned on for 802.1X.

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

Syntax

```
show debugging dot1x
```

Mode User Exec and Privileged Exec

Example To enable 802.1X debugging and display the debugging option set, use the following commands:

```
awplus# debug dot1x
awplus# show debugging dot1x
```

```
802.1X debugging status:
  802.1X events debugging is on
  802.1X timer debugging is on
  802.1X packets debugging is on
  802.1X NSM debugging is on
```

Related commands debug dot1x

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

show dot1x

Overview Use this command to show authentication information for 802.1X port authentication.

If you specify the optional **all** parameter then this command also displays all authentication information for each port available on the switch.

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

Syntax

```
show dot1x [all]
```

Parameter	Description
`all`	Displays all authentication information for each port available on the switch.

Mode Privileged Exec

Example

```
awplus# show dot1x all
```

Table 1: Example output from the **show dot1x all** command

```
awplus# show dot1x all
802.1X Port-Based Authentication Enabled
RADIUS server address: 150.87.18.89:1812
Next radius message id: 5
RADIUS client address: not configured
Authentication info for interface port1.0.2
portEnabled: true - portControl: Auto
portStatus: Authorized
reAuthenticate: disabled
reAuthPeriod: 3600
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
PAE: connectTimeout: 30
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in
KT: keyTxEnabled: false
critical: disabled
guestVlan: disabled
dynamicVlanCreation: single-dynamic-vlan
multiVlanSession: disabled
assignFailActionRule: deny
hostMode: multi-supplicant
    maxsupplicant: 1024
```

Table 1: Example output from the **show dot1x all** command (cont.)

```
dot1x: enabled
protocolVersion: 1
authMac: enabled
method: PAP
reauthRelearning: disabled
authWeb: enabled
method: PAP
lockCount: 3
packetForwarding: disabled
twoStepAuthentication:
    configured: enabled
    actual: enabled
SupplicantMac: none
supplicantMac: none
Supplicant name: manager
Supplicant address: 00d0.59ab.7037
   authenticationMethod: 802.1X Authentication
   portStatus: Authorized - currentId: 1
   abort:F fail:F start:F timeout:F success:T
   PAE: state: Authenticated - portMode: Auto
   PAE: reAuthCount: 0 - rxRespId: 0
   PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
   BE: state: Idle - reqCount: 0 - idFromServer: 0
   CD: adminControlledDirections: in - operControlledDirections: in
   CD: bridgeDetected: false
   KR: rxKey: false
   KT: keyAvailable: false - keyTxEnabled: false
   criticalState: off
   dynamicVlanId: 2
802.1X statistics for interface port1.0.2
   EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
   EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
   EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
   EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
   Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
   EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame Src:  00d0.59ab.7037
Authentication session statistics for interface port1.0.2
   session user name: manager
   session authentication method: Remote server
   session time: 19440 secs
   session terminate cause: Not terminated yet
Authentication Diagnostics for interface port1.0.2
   Supplicant address: 00d0.59ab.7037
   authEnterConnecting: 2
   authEaplogoffWhileConnecting: 1
   authEnterAuthenticating: 2
   authSuccessWhileAuthenticating: 1
   authTimeoutWhileAuthenticating: 1
   authFailWhileAuthenticating: 0
   authEapstartWhileAuthenticating: 0
```

Table 1: Example output from the **show dot1x all** command (cont.)

```
    authEaplogoggWhileAuthenticating: 0
    authReauthsWhileAuthenticated: 0
    authEapstartWhileAuthenticated: 0
    authEaplogoffWhileAuthenticated: 0
    BackendResponses: 2
    BackendAccessChallenges: 1
    BackendOtherrequestToSupplicant: 3
    BackendAuthSuccess: 1
    BackendAuthFails: 0
```

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

show dot1x diagnostics

Overview This command shows 802.1X authentication diagnostics for the specified interface (optional).

If no interface is specified then authentication diagnostics are shown for all interfaces.

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

Syntax

```
show dot1x diagnostics [interface <interface-list>]
```

Parameter	Description
`interface`	Specify a port to show.
`<interface-list>`	The interfaces or ports to configure. An interface-list can be: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • a continuous range of interfaces separated by a hyphen (e.g. port1.0.1-port1.0.3) • a comma-separated list (e.g. port1.0.1, port1.0.3-port1.0.4). Do not mix interface types in a list. The specified interfaces must exist.

Mode Privileged Exec

Example See the sample output below showing 802.1X authentication diagnostics for port1.0.2:

```
awplus# show dot1x diagnostics interface port1.0.2
```

Output Figure 43-1: Example output from the **show dot1x diagnostics** command

```
Authentication Diagnostics for interface port1.0.2
   Supplicant address: 00d0.59ab.7037
      authEnterConnecting: 2
      authEaplogoffWhileConnecting: 1
      authEnterAuthenticating: 2
      authSuccessWhileAuthenticating: 1
      authTimeoutWhileAuthenticating: 1
      authFailWhileAuthenticating: 0
      authEapstartWhileAuthenticating: 0
      authEaplogoggWhileAuthenticating: 0
      authReauthsWhileAuthenticated: 0
      authEapstartWhileAuthenticated: 0
      authEaplogoffWhileAuthenticated: 0
      BackendResponses: 2
      BackendAccessChallenges: 1
      BackendOtherrequestToSupplicant: 3
      BackendAuthSuccess: 1
```

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

show dot1x interface

Overview Use this command to show the status of 802.1X port-based authentication on the specified interface.

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

Syntax

```
show dot1x interface <interface-list>
```

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • a continuous range of interfaces separated by a hyphen (e.g. port1.0.1-port1.0.3) • a comma-separated list (e.g. port1.0.1, port1.0.3-port1.0.4). Do not mix interface types in a list.

Mode Privileged Exec

Examples See the sample output below showing 802.1X authentication status for port1.0.2:

```
awplus# show dot1x interface port1.0.2
```

Table 2: Example output from the **show dot1x interface** command for a port

```
awplus#show dot1x interface port1.0.2
Authentication info for interface port1.0.2
   portEnabled: true - portControl: Auto
   portStatus: Authorized
   reAuthenticate: disabled
   reAuthPeriod: 3600
   PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
   PAE: connectTimeout: 30
   BE: suppTimeout: 30 - serverTimeout: 30
   CD: adminControlledDirections: in
   KT: keyTxEnabled: false
   critical: disabled
   guestVlan: disabled
   dynamicVlanCreation: single-dynamic-vlan
       assignFailActionRule: deny
   multiVlanSession: disabled
   hostMode: multi-supplicant
        maxsupplicant: 1024
   dot1x: enabled
protocolVersion: 1
authMac: enabled
method: PAP
reauthRelearning: disabled
authWeb: enabled
method: PAP
lockCount: 3
packetForwarding: disabled
    twoStepAuthentication:
       configured: enabled
       actual: enabled
supplicantMac: none
```

Related commands

show auth diagnostics

show dot1x sessionstatistics

show dot1x statistics interface

show dot1x supplicant interface

Command changes

Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

show dot1x sessionstatistics

Overview This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

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

Syntax

```
show dot1x sessionstatistics [interface <interface-list>]
```

Parameter	Description
`interface`	Specify a port to show.
<interface-list>	The interfaces to display information about. An interface-list can be: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • a continuous range of interfaces separated by a hyphen (e.g. port1.0.1-port1.0.3) • a comma-separated list (e.g. port1.0.1, port1.0.3-port1.0.4). Do not mix interface types in a list.

Mode Privileged Exec

Example See sample output below showing 802.1X authentication session statistics for port1.0.2:

```
awplus# show dot1x sessionstatistics interface port1.0.2
```

```
Authentication session statistics for interface port1.0.2
   session user name: manager
      session authentication method: Remote server
      session time: 19440 secs
      session terminat cause: Not terminated yet
```

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

show dot1x statistics interface

Overview Use this command to show the authentication statistics for the specified interface.

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

The output from this command is the same as the output from the show auth statistics interface command.

Syntax

```
show dot1x statistics interface <interface-list>
```

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • a continuous range of interfaces separated by a hyphen (e.g. port1.0.1-port1.0.3) • a comma-separated list (e.g. port1.0.1, port1.0.3-port1.0.4). Do not mix interface types in a list.

Mode Privileged Exec

Example To display 802.1X authentication statistics for port1.0.2, use the command:

```
awplus# show dot1x statistics interface port1.0.2
```

Output Figure 43-2: Example output from **show dot1x statistics interface** for a port

```
awplus# show dot1x statistics interface port1.0.2
802.1X statistics for interface port1.0.2
   EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
   EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
   EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
   EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
   Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
   EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame
Src:00d0.59ab.7037
```

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

show dot1x supplicant

Overview This command shows the supplicant state of the authentication mode set for the switch.

This command shows a summary when the optional **brief** parameter is used.

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

Syntax

```
show dot1x supplicant [<macadd>] [brief]
```

Parameter	Description
<macadd>	MAC (hardware) address of the Supplicant.
`brief`	Brief summary of the Supplicant state.

Mode Privileged Exec

Example See sample output below showing the 802.1X authenticated supplicant on the switch:

```
awplus# show dot1x supplicant
```

```
authenticationMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0
Supplicant name: manager
Supplicant address: 00d0.59ab.7037
   authenticationMethod: dot1x
    Two-Step Authentication:
      firstAuthentication: Pass - Method: mac
      secondAuthentication: Pass - Method: dot1x
portStatus: Authorized - currentId: 4
abort:F fail:F start:F timeout:F success:T
PAE: state: Authenticated - portMode: Auto
PAE: reAuthCount: 0 - rxRespId: 0
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 3
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
RADIUS server group (auth): radius
RADIUS server (auth): 192.168.1.40
```

See sample output below showing the supplicant on the switch using the **brief** parameter:

```
awplus# show dot1x supplicant 00d0.59ab.7037 brief
```

```
Interface port1.0.2
   authenticationMethod: dot1x
   totalSupplicantNum: 1
   authorizedSupplicantNum: 1
      macBasedAuthenticationSupplicantNum: 0
      dot1xAuthenticationSupplicantNum: 1
      webBasedAuthenticationSupplicantNum: 0
Interface   VID Mode MAC Address       Status          IP Address      Username
==========  === ==== ===============  =============  ==============  ========
port1.0.2   2   D    00d0.59ab.7037   Authenticated  192.168.2.201   manager
```

See sample output below showing the supplicant on the switch using the **brief** parameter:

```
awplus# show dot1x supplicant brief
```

For example, if two-step authentication is configured with 802.1X authentication as the first method and web authentication as the second method then the output is as follows:

```
Interface port1.0.2  authenticationMethod: dot1x/web
  Two-Step Authentication
    firstMethod: dot1x
    secondMethod: web
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 0
    webBasedAuthenticationSupplicantNum: 1
    otherAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address    Status            IP Address      Username
=========== ==== ==== ============== ================= =============== ========
port1.0.2   5    W    0008.0d5e.c216 Authenticated     192.168.1.200   web
```

Related commands show dot1x supplicant interface

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

show dot1x supplicant interface

Overview Use this command to show the supplicant state of the authentication mode set for the interface.

This command shows a summary when the optional **brief** parameter is used.

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

Syntax

```
show dot1x supplicant interface <interface-list> [brief]
```

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • a continuous range of interfaces separated by a hyphen (e.g. port1.0.1-port1.0.3) • a comma-separated list (e.g. port1.0.1, port1.0.3-port1.0.4). Do not mix interface types in a list.
`brief`	Brief summary of the Supplicant state.

Mode Privileged Exec

Examples See sample output below showing the supplicant on the interface port1.0.2:

```
awplus# show dot1x supplicant interface port1.0.2
```

```
Interface port1.0.2
 authenticationMethod: dot1x
  totalSupplicantNum: 1
 authorizedSupplicantNum: 1
   macBasedAuthenticationSupplicantNum: 0
   dot1xAuthenticationSupplicantNum: 1
   webBasedAuthenticationSupplicantNum: 0
   otherAuthenticationSupplicantNum: 0

 Supplicant name: VCSPCVLAN10
 Supplicant address: 0000.cd07.7b60
   authenticationMethod: 802.1X
 Two-Step Authentication:
   firstAuthentication: Pass - Method: mac
   secondAuthentication: Pass - Method: dot1x
   portStatus: Authorized - currentId: 3
   abort:F fail:F start:F timeout:F success:T
   PAE: state: Authenticated - portMode: Auto
   PAE: reAuthCount: 0 - rxRespId: 0
   PAE: quietPeriod: 60 - maxReauthReq: 2
   BE: state: Idle - reqCount: 0 - idFromServer: 2
   CD: adminControlledDirections:in -
operControlledDirections:in
   CD: bridgeDetected: false
   KR: rxKey: false
   KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing the supplicant on the switch using the **brief** parameter:

```
awplus# show dot1x supplicant interface port1.0.2 brief
```

```
Interface port1.0.2
   authenticationMethod: dot1x
Two-Step Authentication:
   firstMethod: mac
   secondMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address     Status          IP Address      Username
=========   ===  ==== ===========     ======          ==========      ========
port1.0.2   2    D    00d0.59ab.7037  Authenticated   192.168.2.201   manager
```

Related commands show dot1x supplicant

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

undebug dot1x

Overview This command applies the functionality of the **no** variant of the debug dot1x command.

44 Authentication Commands

Introduction

Overview

Port authentication commands enable you to specify three different types of device authentication: 802.1X authentication, web authentication, and MAC authentication.

- 802.1X is an IEEE standard providing a mechanism for authenticating devices attached to a LAN port or wireless device.
- Web authentication is applicable to devices that have a human user who opens the web browser and types in a user name and password when requested.
- MAC authentication is used to authenticate devices that have neither a human user nor implement 802.1X supplicant when making a network connection request.

This chapter provides an alphabetical reference for MAC and web authentication commands. For a list of 802.1X commands see the 802.1X Commands chapter.

For more information on configuring and using port authentication, see the AAA and Port Authentication Feature Overview and Configuration Guide.

Command List

- "auth auth-fail vlan" on page 2166
- "auth critical" on page 2168
- "auth dhcp-framed-ip-lease" on page 2169
- "auth dynamic-vlan-creation" on page 2171
- "auth guest-vlan" on page 2174
- "auth guest-vlan forward" on page 2176
- "auth guest-vlan hw-forwarding" on page 2178
- "auth host-mode" on page 2179
- "auth log" on page 2181
- "auth max-supplicant" on page 2183

- "auth multi-vlan-session" on page 2185
- "auth priority" on page 2186
- "auth profile (global)" on page 2188
- "auth profile (interface)" on page 2189
- "auth reauthentication" on page 2190
- "auth roaming disconnected" on page 2191
- "auth roaming enable" on page 2193
- "auth supplicant-ip" on page 2195
- "auth supplicant-mac" on page 2197
- "auth timeout connect-timeout" on page 2200
- "auth timeout quiet-period" on page 2201
- "auth timeout reauth-period" on page 2202
- "auth timeout server-timeout" on page 2204
- "auth timeout supp-timeout" on page 2206
- "auth two-step enable" on page 2207
- "auth two-step order" on page 2210
- "auth-mac accounting" on page 2212
- "auth-mac authentication" on page 2213
- "auth-mac enable" on page 2214
- "auth-mac method" on page 2216
- "auth-mac password" on page 2218
- "auth-mac reauth-relearning" on page 2219
- "auth-mac static" on page 2220
- "auth-mac username" on page 2221
- "auth-web accounting" on page 2222
- "auth-web authentication" on page 2223
- "auth-web enable" on page 2224
- "auth-web forward" on page 2226
- "auth-web idle-timeout enable" on page 2229
- "auth-web idle-timeout timeout" on page 2230
- "auth-web max-auth-fail" on page 2231
- "auth-web method" on page 2233
- "auth-web-server blocking-mode" on page 2234
- "auth-web-server dhcp ipaddress" on page 2235
- "auth-web-server dhcp lease" on page 2236

- "auth-web-server dhcp-wpad-option" on page 2237
- "auth-web-server host-name" on page 2238
- "auth-web-server intercept-port" on page 2239
- "auth-web-server ipaddress" on page 2240
- "auth-web-server page language" on page 2241
- "auth-web-server login-url" on page 2242
- "auth-web-server page logo" on page 2243
- "auth-web-server page sub-title" on page 2244
- "auth-web-server page success-message" on page 2245
- "auth-web-server page title" on page 2246
- "auth-web-server page welcome-message" on page 2247
- "auth-web-server ping-poll enable" on page 2248
- "auth-web-server ping-poll failcount" on page 2249
- "auth-web-server ping-poll interval" on page 2250
- "auth-web-server ping-poll reauth-timer-refresh" on page 2251
- "auth-web-server ping-poll timeout" on page 2252
- "auth-web-server port" on page 2253
- "auth-web-server redirect-delay-time" on page 2254
- "auth-web-server redirect-url" on page 2255
- "auth-web-server session-keep" on page 2256
- "auth-web-server ssl" on page 2257
- "auth-web-server ssl intercept-port" on page 2258
- "copy proxy-autoconfig-file" on page 2259
- "copy web-auth-https-file" on page 2260
- "description (auth-profile)" on page 2261
- "erase proxy-autoconfig-file" on page 2262
- "erase web-auth-https-file" on page 2263
- "platform l3-vlan-hashing-algorithm" on page 2264
- "platform mac-vlan-hashing-algorithm" on page 2265
- "show auth" on page 2266
- "show auth diagnostics" on page 2268
- "show auth interface" on page 2270
- "show auth sessionstatistics" on page 2272
- "show auth statistics interface" on page 2273
- "show auth supplicant" on page 2274

- "show auth supplicant interface" on page 2277
- "show auth two-step supplicant brief" on page 2278
- "show auth-web-server" on page 2280
- "show auth-web-server page" on page 2281
- "show proxy-autoconfig-file" on page 2282

auth auth-fail vlan

Overview Use this command to enable the **auth-fail vlan** feature on the specified vlan interface. This feature assigns supplicants (client devices) to the specified VLAN if they fail port authentication.

Use the **no** variant of this command to disable the auth-fail vlan feature for a specified VLAN interface.

Syntax

```
auth auth-fail vlan <1-4094>
no auth auth-fail vlan
```

Parameter	Description
<1-4094>	Assigns the VLAN ID to any supplicants that have failed port authentication.

Default The auth-fail vlan feature is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes Use the auth-fail vlan feature when using web authentication instead of the Guest VLAN feature, when you need to separate networks where one supplicant (client device) requires authentication and another supplicant does not require authentication from the same interface.

This is because the DHCP lease time using the Web-Authentication feature is shorter, and the auth-fail vlan feature enables assignment to a different VLAN if a supplicant fails authentication.

To enable the auth-fail vlan feature with web authentication, you need to set the web authentication server virtual IP address by using the auth-web-server ipaddress command or the auth-web-server dhcp ipaddress command.

When using 802.1X port authentication, use a dot1x max-auth-fail command to set the maximum number of login attempts. Three login attempts are allowed by default for 802.1X port authentication before supplicants trying to authenticate are moved from the Guest VLAN to the auth-fail VLAN. See the dot1x max-auth-fail on page 2139 for command information.

See the AAA and Port Authentication Feature Overview and Configuration Guide for information about:

- the auth-fail VLAN feature, which allows the Network Administrator to separate the supplicants who attempted authentication, but failed, from the supplicants who did not attempt authentication, and
- restrictions regarding combinations of authentication enhancements working together

Use appropriate ACLs (Access Control Lists) on interfaces for extra security if a supplicant allocated to the designated auth-fail vlan can access the same network

as a supplicant on the Guest VLAN. For more information about ACL concepts, and configuring ACLs see the ACL Feature Overview and Configuration Guide. For more information about ACL commands see:

- IPv4 Hardware Access Control List (ACL) Commands
- IPv4 Software Access Control List (ACL) Commands
- IPv6 Hardware Access Control List (ACL) Commands
- IPv6 Software Access Control List (ACL) Commands

Examples To enable the auth-fail vlan feature for port1.0.2 and assign VLAN 100, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth auth-fail vlan 100
```

To disable the auth-fail vlan feature for port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth auth-fail vlan
```

Related commands

auth profile (global)

dot1x max-auth-fail

show dot1x

show dot1x interface

show running-config

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

auth critical

Overview Use this command to enable the critical port feature on the interface. When the critical port feature is enabled on an interface, and all the RADIUS servers are unavailable, then the interface becomes authorized.

The **no** variant of this command disables the critical port feature on the interface.

Syntax

```
auth critical
no auth critical
```

Default The critical port of port authentication is disabled.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To enable the critical port feature on interface port1.0.2, use the following commands:

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

To disable the critical port feature on interface port1.0.2, use the following commands:

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

To enable the critical port feature on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth critical
```

Related commands

auth profile (global)

show auth-web-server

show dot1x

show dot1x interface

show running-config

auth dhcp-framed-ip-lease

Overview Use this command to enable DHCP Framed IP Lease on an interface.

When the DHCP Framed IP Lease feature is enabled on an interface, supplicants authenticated using 802.1x or MAC authentication will be assigned a specific IP address, and other network settings, gathered from the RADIUS server during the authentication process.

Use the **no** variant of this command to disable DHCP Framed IP Lease.

Syntax

```
auth dhcp-framed-ip-lease
no auth dhcp-framed-ip-lease
```

Default DHCP Framed IP Lease is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes You need to complete the following steps to configure the DHCP Framed IP Lease feature on your network.

On the RADIUS server:

- Configure the RADIUS server with the username and password for 802.1x or MAC authentication
- Configure the following 'framed' RADIUS attributes on the RADIUS server for the that user:
  - Framed-IP-Address (8): the IPv4 address for the supplicant
  - Framed-IP-Netmask (9): the netmask for the supplicant
  - Framed-Route (22): the default gateway IPv4 address for the supplicant
  - Session-Timeout (27): IP address lease time for the supplicant

NOTE: *The Frame-IP-Address (8) attribute must be configured for this feature to work. All other attributes are optional.*

On the DHCP server:

- Configure the RADIUS client
- Enable 802.1x or MAC authentication on the required interface/s
- Enable DHCP Framed IP Lease feature on the required interface/s
- Setup a DHCP pool with the network range for the IP address/es registered on the RADIUS server
- Enable DHCP server

For more information, see the AAA and Port Authentication Feature Overview and Configuration Guide.

Example

To enable DHCP Framed IP Lease on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# auth dhcp-framed-ip-lease
```

To disable DHCP Framed IP Lease on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no auth dhcp-framed-ip-lease
```

Related commands

show dot1x supplicant

show ip dhcp pool

Command changes

Version 5.4.8-2.1: command added

auth dynamic-vlan-creation

Overview Use this command to enable and disable the Dynamic VLAN assignment feature.

The Dynamic VLAN assignment feature allows a supplicant (client device) to be placed into a specific VLAN based on information returned from the RADIUS server during authentication, on a given interface.

Use the **no** variant of this command to disable the Dynamic VLAN assignment feature.

Syntax

```
auth dynamic-vlan-creation [rule {deny|permit}] [type
{multi|single}]
no auth dynamic-vlan-creation
```

Parameter	Description
`rule`	VLAN assignment rule.
`deny`	Deny a differently assigned VLAN ID. This is the default rule.
`permit`	Permit a differently assigned VLAN ID.
`type`	Specifies whether multiple different VLANs can be assigned to supplicants (client devices) attached to the port, or whether only a single VLAN can be assigned to supplicants on the port.
`multi`	Multiple Dynamic VLAN.
`single`	Single Dynamic VLAN.

Default By default, the Dynamic VLAN assignment feature is disabled.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes If the Dynamic VLAN assignment feature is enabled, VLAN assignment is dynamic. If the Dynamic VLAN assignment feature is disabled then RADIUS attributes are ignored and configured VLANs are assigned to ports. Dynamic VLANs may be associated with authenticated MAC addresses if the **type** parameter is applied with the **rule** parameter.

The **rule** parameter deals with the case where there are multiple supplicants attached to a port, and the type parameter has been set to **single-vlan**. The parameter specifies how the switch should act if different VLAN IDs end up being assigned to different supplicants. The keyword value **deny** means that once a given VID has been assigned to the first supplicant, then if any subsequent supplicant is assigned a different VID, that supplicant is rejected. The keyword value **permit** means that once a given VID has been assigned to the first supplicant, then if any subsequent supplicant is assigned a different VID, that supplicant is accepted, but it is actually assigned the same VID as the first supplicant.

If you issue an **auth dynamic-vlan-creation** command without a **rule** parameter then a second supplicant with a different VLAN ID is rejected. It is not assigned to the first supplicant's VLAN. Issuing an **auth dynamic-vlan-creation** command without a **rule** parameter has the same effect as issuing an **auth dynamic-vlan-creation rule deny** command rejecting supplicants with differing VIDs.

The **type** parameter specifies whether multiple different VLANs can be assigned to supplicants attached to the port, or whether only a single VLAN can be assigned to supplicants on the port. The **type** parameter can select the port base VLAN or the MAC base VLAN from the RADIUS VLAN ID. This can be used when the host-mode is set to multi-supplicant. For **single**-host ports, the VLAN ID will be assigned to the port. It is not supported with the Guest VLAN feature. Display the ID assigned using a **show vlan** command. For **multi**-host ports, the VLAN ID will be assigned to the MAC address of the authenticated supplicant. The VLAN ID assigned for the MAC Base VLAN is displayed using the **show platform table vlan** command.

To configure Dynamic VLAN with Web Authentication, you need to set the Web Authentication Server virtual IP address by using the auth-web-server ipaddress command or the auth-web-server dhcp ipaddress command. You also need to create a hardware access-list that can be applied to the switch port interface.

You need to configure an IPv4 address for the VLAN interface on which Web Authentication is running.

Examples To enable the Dynamic VLAN assignment feature on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport access vlan 10
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# interface vlan10
awplus(config-if)# ip address 10.1.1.1/24
```

To enable the Dynamic VLAN assignment feature with Web Authentication on interface port1.0.2 when Web Authentication is needed, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ipaddress 1.2.3.4
awplus(config)# access-list hardware acl-web send-to-cpu ip any
1.2.3.4
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# access-group acl-web
awplus(config-if)# interface vlan1
awplus(config-if)# ip address 10.1.1.1/24
```

To disable the Dynamic VLAN assignment feature on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth dynamic-vlan-creation
```

To enable the Dynamic VLAN assignment feature on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth dynamic-vlan-creation
```

Related commands

auth profile (global)

auth host-mode

show dot1x

show dot1x interface

show running-config

Command changes

Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

auth guest-vlan

Overview Use this command to enable and configure the Guest VLAN feature on the interface specified by associating a Guest VLAN with an interface. This command does not start authentication. The supplicant's (client device's) traffic is associated with the native VLAN of the interface unless it is already associated with another VLAN. The **routing** option enables routing from the Guest VLAN to another VLAN, so the switch can lease DHCP addresses and accept access to a limited network.

The **no** variant of this command disables the guest VLAN feature on the interface specified.

Syntax

```
auth guest-vlan <1-4094> [routing]
no auth guest-vlan [routing]
```

Parameter	Description
<1-4094>	VLAN ID (VID).
`routing`	Enables routing from the Guest VLAN to other VLANs.

Default The Guest VLAN authentication feature is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes The Guest VLAN feature may be used by supplicants (client devices) that have not attempted authentication, or have failed the authentication process. Note that if a port is in multi-supplicant mode with per-port dynamic VLAN configuration, after the first successful authentication, subsequent hosts cannot use the guest VLAN due to the change in VLAN ID. This may be avoided by using per-user dynamic VLAN assignment.

When using the Guest VLAN feature with the multi-host mode, a number of supplicants can communicate via a guest VLAN before authentication. A supplicant's traffic is associated with the native VLAN of the specified switch port. The supplicant must belong to a VLAN before traffic from the supplicant can be associated.

Note that you must enable 802.1X on the port and define a VLAN using the vlan command before you can configure it as a guest VLAN.

Roaming Authentication cannot be enabled if DHCP snooping is enabled (service dhcp-snooping command), and vice versa.

Note that Guest VLAN can use only untagged ports.

See the AAA and Port Authentication Feature Overview and Configuration Guide for information about:

- Guest VLAN, and

- restrictions regarding combinations of authentication enhancements working together

Examples

To define vlan100 and assign the guest VLAN feature to vlan100 on interface port1.0.2, and enable routing from the guest VLAN to other VLANs, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 100
awplus(config-vlan)# exit
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth guest-vlan 100 routing
```

To disable the guest VLAN feature on port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth guest-vlan
```

To define vlan100 and assign the guest VLAN feature to vlan100 on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 100
awplus(config-vlan)# exit
awplus(config)# auth profile student
awplus(config-auth-profile)# auth guest-vlan 100
```

Related commands

auth profile (global)

auth guest-vlan forward

dot1x port-control

show dot1x

show dot1x interface

Command changes

Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

auth guest-vlan forward

Overview Use this command to enable packet forwarding from the guest VLAN to a destination IP address or subnet. If this command is configured, the device can lease DHCP addresses and accept access to a limited part of your network. Also, when using NAP authentication, the supplicant can log on to a domain controller to gain certification.

Use the **no** variant of this command to disable packet forwarding from the Guest VLAN to a destination IP address or subnet.

Syntax

```
auth guest-vlan forward {<ip-address>|<ip-address/mask>}
[dns|tcp <1-65535>|udp <1-65535>]
```

```
no auth guest-vlan forward {<ip-address>|<ip-address/mask>}
[dns|tcp <1-65535>|udp <1-65535>]
```

Parameter	Description
<ip-address> <ip-address/mask>	The IP address or subnet to which the guest VLAN can forward packets, in dotted decimal notation
`dns`	Enable forwarding of DNS packets
`tcp <1-65535>`	Enable forwarding of packets for the specified TCP port number
`udp <1-65535>`	Enable forwarding of packets for the specified UDP port number

Default Forwarding is disabled by default.

Mode Interface Configuration mode for a specified switch port, or Authentication Profile mode

Usage Before using this command, you must configure the guest VLAN with the auth guest-vlan command.

Example To enable packet forwarding from the guest VLAN to the destination IP address on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth guest-vlan forward 10.0.0.1
```

To enable forwarding of DNS packets from the guest VLAN to the destination IP address on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface
awplus(config-if)# auth guest-vlan forward 10.0.0.1 dns
```

To disable forwarding of DNS packets from the guest VLAN to the destination IP address on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth guest-vlan forward 10.0.0.1 dns
```

To enable the TCP forwarding port 137 on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth guest-vlan forward 10.0.0.1
tcp 137
```

Related commands

auth guest-vlan

auth profile (global)

show running-config

Command changes

Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

auth guest-vlan hw-forwarding

Overview Use this command to enable hardware forwarding on the guest VLAN. By default, hardware forwarding is disabled and all traffic on the VLAN is forwarded by the CPU.

Use the **no** variant of this command to disable hardware forwarding on the guest VLAN.

Syntax
```
auth guest-vlan hw-forwarding
no auth guest-vlan hw-forwarding
```

Default Disabled.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To enable guest VLAN hardware forwarding on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth guest-vlan hw-forwarding
```

To disable guest VLAN hardware forwarding on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth guest-vlan hw-forwarding
```

To enable guest VLAN hardware forwarding authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth guest-vlan hw-forwarding
```

Related commands
auth profile (global)

auth guest-vlan

auth guest-vlan forward

Command changes Version 5.5.0-1.1: command added to x230, GS970M, IE210 series switches.

Version 5.5.1-0.1: command added to all other AlliedWare Plus switches.

auth host-mode

Overview Use this command to select the host mode on the specified interface.

Use the **no** variant of this command to set host mode to the default setting (single host).

Syntax

```
auth host-mode {single-host|multi-host|multi-supplicant}
no auth host-mode
```

Parameter	Description
`single-host`	In this mode, only one supplicant is allowed per port. This is the default mode.
`multi-host`	In this mode, once the first host on a port is authenticated, all other downstream hosts are allowed without being authenticated (piggy-back mode).
`multi-supplicant`	In this mode, multiple separate supplicants are individually authenticated on one port.

Default The default host mode for port authentication is for a single host.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes

Single-host mode

With this mode, only one supplicant may be authenticated on the port. Once that host has been authenticated, no other supplicants may be authenticated until the first supplicant's session has closed. This means, of course, that none of the other hosts downstream of the port will be able to send or receive traffic on that port.

This option is recommended when you know that there should only be one host connected to a port. By limiting the port to a single authenticated host, you guard against the consequences of someone accidentally or maliciously connecting a downstream switch to the port.

Multi-host mode

With this mode, once the first host has been authenticated on the port, all other downstream hosts are allowed without being authenticated. This is sometimes known as piggy-back mode. It is useful when the downstream switch attached to the authenticating port is an intelligent switch that can act as an authentication supplicant.

If you trust that malicious users cannot be connected to that switch but you do not know the identity of those users, then you can simply authenticate the switch and then allow its attached users to have network access. If the valid switch is disconnected and an invalid one is connected which is not configured with the correct authentication credentials, then the devices connected to the invalid switch will be blocked from accessing the network.

Examples

To set the host mode to multi-supplicant on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth host-mode multi-supplicant
```

To set the host mode to default (single host) on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth host-mode
```

To set the host mode to multi-supplicant on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth host-mode multi-supplicant
```

To set the host mode to default (single host) on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth host-mode
```

Related commands

auth profile (global)

show dot1x

show dot1x interface

show running-config

auth log

Overview Use this command to configure the types of authentication feature log messages that are output to the log file.

Use the **no** variant of this command to remove either specified types or all types of authentication feature log messages that are output to the log file.

Syntax

```
auth log {dot1x|auth-mac|auth-web}
{success|failure|logoff|all}
```

```
no auth log {dot1x|auth-mac|auth-web}
{success|failure|logoff|all}
```

Parameter	Description
`dot1x`	Specify only 802.1X-Authentication log messages are output to the log file.
`auth-mac`	Specify only MAC-Authentication log messages are output to the log file.
`auth-web`	Specify only Web-Authentication log messages are output to the log file.
`success`	Specify only successful authentication log messages are output to the log file.
`failure`	Specify only authentication failure log messages are output to the log file.
`logoff`	Specify only authentication log-off messages are output to the log file. Note that link down, age out and expired ping polling messages will be included.
`all`	Specify all types of authentication log messages are output to the log file. Note that this is the default behavior for the authentication logging feature.

Default All types of authentication log messages are output to the log file by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To configure the logging of MAC authentication failures to the log file for supplicants (client devices) connected to interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth log auth-mac failure
```

To disable the logging of all types of authentication log messages to the log file for auth-mac supplicants (client devices) connected to interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth log auth-mac all
```

To configure the logging of web authentication failures to the log file for supplicants (client devices) connected to authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth log auth-web failure
```

To disable the logging of all types of authentication log messages to the log file for auth-mac supplicants (client devices) connected to authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth log auth-mac all
```

Related commands

auth profile (global)

show running-config

auth max-supplicant

Overview Use this command to set the maximum number of supplicants (client devices) that can be authenticated on the selected port. Once this value is exceeded, further supplicants will not be authenticated.

The **no** variant of this command resets the maximum supplicant number to the default.

Syntax

```
auth max-supplicant <2-1024>
no auth max-supplicant
```

Parameter	Description
<2-1024>	Limit number.

Default The max supplicant of port authentication is 1024.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the maximum number of supplicants to 10 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth max-supplicant 10
```

To reset the maximum number of supplicants to the default value on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth max-supplicant
```

To set the maximum number of supplicants to 10 on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth max-supplicant 10
```

To reset the maximum number of supplicants to the default value on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth max-supplicant
```

Related commands

auth profile (global)

show dot1x

show dot1x interface

show running-config

auth multi-vlan-session

Overview Use this command to enable packet forwarding on multiple VLANs for an authenticated supplicant attached to a trunked (tagged VLAN) port.

By default, AlliedWare Plus only allows packet forwarding on the VLAN that a device was authenticated on. This command enables packet forwarding to the attached device on any VLAN configured on the switchport. After the device authenticates it will have access to all VLANs configured on the switchport.

Use the **no** variant of this command to disable packet forwarding on multiple VLANs for an authenticated supplicant.

Syntax

```
auth multi-vlan-session
no auth multi-vlan-session
```

Default By default, **multi-vlan-session** is disabled.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To allow a client attached to port1.0.2 to access all VLANs configured on the AlliedWare Plus device, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan all
awplus(config-if)# auth host-mode multi-supplicant
awplus(config-if)# auth multi-vlan-session
```

To disable **multi-vlan-session** on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth multi-vlan-session
```

Related commands

auth-mac enable

auth-web enable

dot1x port-control

show auth interface

show dot1x interface

Command changes Version 5.4.8-1.1: command added

Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

auth priority

Overview Use this command to enable authentication priority on an interface. This sets the tri-authentication order of priority for MAC, 802.1X, and web-based authentication. If tri-authentication is not configured on the interface then this command has no effect.

You specify the authentication methods in order of priority. The first method in the list has the highest priority, the second method has the second highest priority, and the third method has the lowest priority. Any methods not specified will have the lowest priority.

Use the **no** variant of this command to disable authentication priority.

Syntax

```
auth priority {[auth-mac] [dot1x] [auth-web]}
no auth priority
```

Parameter	Description
`auth-mac`	Set MAC authentication priority.
`dot1x`	Set 802.1X authentication priority.
`auth-web`	Set web-based authentication priority.

Default Authentication priority is not set.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes Before using this command you must correctly configure tri-authentication on the interface. Tri-authentication is when multiple authentication methods (MAC, 802.1X, and/or web-based) are configured on the same interface. With tri-authentication, a supplicant is authorized to use the network as soon as they are successfully authenticated by any of the configured authentication methods.

When authentication priority is not set, once a supplicant is authenticated any future attempts to authenticate are ignored. When, however, authentication priority is set, and a higher priority authentication attempt is made by the supplicant, a new authentication process starts. The supplicant will then be authorized, or unauthorized, based on the result of this new authentication attempt.

Example

To configure 802.1X authentication to have a higher priority than MAC authentication on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth priority dot1x auth-mac
```

To disable authentication priority on interface port1.0.2, use the commands:

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

To configure 802.1X authentication to have a higher priority than MAC authentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth priority dot1x auth-mac
```

Related commands

auth profile (interface)

auth-mac enable

auth-web enable

dot1x port-control

Command changes

Version 5.5.0-2.1: command added

auth profile (global)

Overview Use this command to enter port authentication profile mode and configure a port authentication profile.

If the specified profile does not exist a new authentication profile is created with the name provided.

Use the **no** variant of this command to delete the specified port authentication profile.

Syntax

```
auth profile <profile-name>
no auth profile <profile-name>
```

Parameter	Description
<profile-name>	Name of the profile to create or configure.

Default No port authentication profiles are created by default.

Mode Global Configuration

Usage A port authentication profile is a configuration object that aggregates multiple port authentication commands. These profiles are attached or detached from an interface using the auth profile (interface) command.

Example To create a new authentication profile 'student', use the following commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)#
```

To delete an authentication profile 'student', use the following commands:

```
awplus# configure terminal
awplus(config)# no auth profile student
```

Related commands auth profile (interface)

description (auth-profile)

auth profile (interface)

Overview Use this command to attach a port authentication profile to the current interface.

Use the **no** variant of this command to detach a port authentication profile from the current interface.

Syntax

```
auth profile <profile-name>
no auth profile <profile-name>
```

Parameter	Description
<profile-name>	The name of the profile to attach to the current interface.

Default No profile is attached by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage This command attaches an authentication profile, that was created using the auth profile (global) command, to a static channel, a dynamic (LACP) channel group, or a switch port.

You can only attach one profile to an interface at a time. Use the **no** variant of the command to detach a profile before attempting to attach another one.

Example To attach the authentication profile 'student' to port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth profile student
```

To detach the authentication profile 'student' from port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth profile student
```

Related commands auth profile (global)

auth reauthentication

Overview Use this command to enable re-authentication on the interface specified in the Interface mode, which may be a static channel group (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the **no** variant of this command to disable reauthentication on the interface.

Syntax

```
auth reauthentication
no auth reauthentication
```

Default Reauthentication of port authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To enable reauthentication on interface port1.0.2, use the following commands:

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

To disable reauthentication on interface port1.0.2, use the following commands:

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

To enable reauthentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth reauthentication
```

Related commands

auth profile (global)

show dot1x

show dot1x interface

show running-config

auth roaming disconnected

Overview This command allows a supplicant to move to another authenticating interface without reauthentication, even if the link is down for the interface that the supplicant is currently connected to.

You must enter the auth roaming enable command on both interfaces before using this command.

The **no** variant of this command disables roaming authentication on interfaces that are link-down, and forces a supplicant to be reauthenticated when moving between interfaces.

See the AAA and Port Authentication Feature Overview and Configuration Guide for further information about this feature.

Syntax

```
auth roaming disconnected
no auth roaming disconnected
```

Default By default, the authentication status for a roaming supplicant is deleted when an interface goes down, so supplicants must reauthenticate.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes Note that 802.1X port authentication, MAC-authentication, or Web-authentication must be configured before using this feature. The port that the supplicant is moving to must have the same authentication configuration as the port the supplicant is moving from.

Roaming Authentication cannot be enabled if DHCP snooping is enabled (service dhcp-snooping command), and vice versa.

Examples To allow supplicants to move from port1.0.2 without reauthentication even when the link is down, when using 802.1X authentication, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth roaming enable
awplus(config-if)# auth roaming disconnected
```

To require supplicants to reauthenticate when moving from port1.0.2 if the link is down, when using 802.1X authentication, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth roaming disconnected
```

To allow supplicants using authentication profile 'student' to move between ports without reauthentication even when the link is down, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth roaming disconnected
```

To require supplicants using authentication profile 'student' to reauthenticate when moving between ports if the link is down, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth roaming disconnected
```

Related commands

auth profile (global)

auth-mac enable

auth roaming enable

auth-web enable

dot1x port-control

show auth interface

show dot1x interface

show running-config

auth roaming enable

Overview Use this command to allow a supplicant to move to another authenticating interface without reauthentication, providing the link is up for the interface that the supplicant is currently connected to.

The **no** variant of this command disables roaming authentication on an interface, and forces a supplicant to be reauthenticated when moving between interfaces.

See the AAA and Port Authentication Feature Overview and Configuration Guide for further information about this feature.

Syntax

```
auth roaming enable
no auth roaming enable
```

Default Roaming authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes Note that 802.1X port authentication, MAC authentication, or web-based authentication must be configured before using this feature. The port that the supplicant is moving to must have the same authentication configuration as the port the supplicant is moving from.

This command only enables roaming authentication for links that are up. If you want roaming authentication on links that are down, you must also use the command auth roaming disconnected.

Roaming Authentication cannot be enabled if DHCP snooping is enabled (service dhcp-snooping command), and vice versa.

Examples To enable roaming authentication for port1.0.4, when using auth-mac authentication, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# auth-mac enable
awplus(config-if)# auth roaming enable
```

To disable roaming authentication for port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no auth roaming enable
```

To enable roaming authentication for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth roaming enable
```

Related commands

auth profile (global)

auth-mac enable

auth roaming disconnected

auth-web enable

dot1x port-control

show auth interface

show dot1x interface

show running-config

auth supplicant-ip

Overview Use this command to add a supplicant (client device) IP address on a given interface and provides parameters for its configuration.

Use the **no** variant of this command to delete the supplicant IP address and reset other parameters to their default values. The IP address can be determined before authentication for auth-web clients only.

Syntax

```
auth supplicant-ip <ip-addr> [max-reauth-req <1-10>]
[port-control {auto|force-authorized|force-unauthorized|
skip-second-auth}] [quiet-period <1-65535>] [reauth-period
<1-4294967295>] [supp-timeout <1-65535>] [server-timeout
<1-65535>] [reauthentication]
```

```
no auth supplicant-ip <ip-addr> [reauthentication]
```

Parameter	Description
<ip-addr>	IP address of the supplicant entry in A.B.C.D/P format.
`max-reauth-req`	The number of reauthentication attempts before becoming unauthorized.
<1-10>	Count of reauthentication attempts (default 2).
`port-control`	Port control commands.
`auto`	A port control parameter that allows port clients to negotiate authentication.
`force-authorized`	A port control parameter that forces the port state to authorized.
`force-unauthorized`	A port control parameter that forces the port state to unauthorized.
`skip-second-auth`	Skip the second authentication.
`quiet-period`	Quiet period during which the port remains in the HELD state (default 60 seconds).
<1-65535>	Seconds for quiet period.
`reauth-period`	Seconds between reauthorization attempts (default 3600 seconds).
<1-4294967295>	Seconds for reauthorization attempts (reauth-period).
`supp-timeout`	Supplicant response timeout.
<1-65535>	Seconds for supplicant response timeout (default 30 seconds).
`server-timeout`	The period, in seconds, before the authentication server response times out.

Parameter	Description
<1-65535>	The server-timeout period, in seconds, default 3600 seconds.
`reauthentication`	Enable reauthentication on a port.

Default No supplicant IP address for port authentication exists by default until first created with the **auth supplicant-ip** command. The defaults for parameters applied are as shown in the table above.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To add the supplicant IP address 192.168.10.0/24 to force authorized port control for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth supplicant-ip 192.168.10.0/24
port-control force-authorized
```

To delete the supplicant IP address 192.168.10.0/24 for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth supplicant-ip 192.168.10.0/24
```

To disable reauthentication for the supplicant(s) IP address 192.168.10.0/24 for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth supplicant-ip 192.168.10.0/24
reauthentication
```

To add the supplicant IP address 192.168.10.0/24 to force authorized port control for auth profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth supplicant-ip
192.168.10.0/24 port-control force-authorized
```

Related commands

show auth

show dot1x

show dot1x interface

show running-config

auth supplicant-mac

Overview This command adds a supplicant (client device) MAC address or MAC mask on a given interface with the parameters as specified in the table below.

Use the **no** variant of this command to delete the supplicant MAC address and reset other parameters to their default values.

Syntax

```
auth supplicant-mac <mac-addr> [mask <mac-addr-mask>]
[max-reauth-req <1-10>] [port-control {auto|force-authorized|
force-unauthorized|skip-second-auth}] [quiet-period <1-65535>]
[reauth-period <1-4294967295>] [supp-timeout <1-65535>]
[server-timeout <1-65535>] [reauthentication]
```

```
no auth supplicant-mac <mac-addr> [reauthentication]
```

Parameter	Description
<mac-addr>	MAC (hardware) address of the supplicant entry in HHHH.HHHH.HHHH MAC address hexadecimal format.
`mask`	A mask applied to MAC addresses in order to select only those addresses containing a specific string.
<mac-addr-mask>	The mask comprises a string of three (period separated) bytes, where each byte comprises four hexadecimal characters that will generally be either 1or 0. When the mask is applied to a specific MAC address, a match is only required for characters that correspond to a 1 in the mask. Characters that correspond to a 0 in the mask are effectively ignored. In the examples section below, the mask ffff.ff00.0000 is applied for the MAC address 0000.5E00.0000. The applied mask will then match only those MAC addresses that begin with 0000.5E (in this case the OUI component). The remaining portion of the addresses (in this case the NIC component) will be ignored.
`port-control`	Port control commands.
`auto`	Allow port client to negotiate authentication.
`force-authorized`	Force port state to authorized.
`force-unauthorized`	Force port state to unauthorized.
`skip-second-auth`	Skip the second authentication.
`quiet-period`	Quiet period in the HELD state (default 60 seconds).
<1-65535>	Seconds for quiet period.
`reauth-period`	Seconds between reauthorization attempts (default 3600 seconds).
<1-4294967295>	Seconds for reauthorization attempts (reauth-period).
`supp-timeout`	Supplicant response timeout (default 30 seconds).

Parameter	Description
<1-65535>	Seconds for supplicant response timeout.
`server-timeout`	Authentication server response timeout (default 30 seconds).
<1-65535>	Seconds for authentication server response timeout.
`reauthentication`	Enable reauthentication on a port.
`max-reauth-req`	No of reauthentication attempts before becoming unauthorized (default 2).
<1-10>	Count of reauthentication attempts.

Default No supplicant MAC address for port authentication exists by default until first created with the **auth supplicant-mac** command. The defaults for parameters are shown in the table above.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To add the supplicant MAC address 0000.5E00.5343 to force authorized port control for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth supplicant-mac 0000.5E00.5343
port-control force-authorized
```

To apply the mask ffff.ff00.0000 in order to add any supplicant MAC addresses whose MAC address begins with 0000.5E, and then to force authorized port control for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth supplicant-mac 0000.5E00.0000 mask
ffff.ff00.0000 port-control force-authorized
```

To delete the supplicant MAC address 0000.5E00.5343 for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth supplicant-mac 0000.5E00.5343
```

To disable reauthentication for the supplicant MAC address 0000.5E00.5343 for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth supplicant-mac 0000.5E00.5343
reauthentication
```

To add the supplicant MAC address 0000.5E00.5343 to force authorized port control for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth supplicant-mac
0000.5E00.5343 port-control force-authorized
```

To delete the supplicant MAC address 0000.5E00.5343 for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth supplicant-mac
0000.5E00.5343
```

Related commands

show auth

show dot1x

show dot1x interface

show running-config

auth timeout connect-timeout

Overview Use this command to set the connect-timeout period for the interface.

Use the **no** variant of this command to reset the connect-timeout period to the default.

Syntax

```
auth timeout connect-timeout <1-65535>
no auth timeout connect-timeout
```

Parameter	Description
<1-65535>	Specifies the connect-timeout period (in seconds).

Default The connect-timeout default is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes This command is used for MAC and web authentication. If the connect-timeout has lapsed and the supplicant has the state **connecting**, then the supplicant is deleted. When auth-web-server session-keep or auth two-step enable is enabled, we recommend you configure a longer connect-timeout period.

Examples To set the connect-timeout period to 3600 seconds for port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout connect-timeout 3600
```

To reset the connect-timeout period to the default (30 seconds) for port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout connect-timeout
```

To set the connect-timeout period to 3600 seconds for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth timeout connect-timeout 3600
```

Related commands auth profile (global)

show dot1x

show dot1x interface

auth timeout quiet-period

Overview Use this command to set a time period for which another authentication request is not accepted on a given interface, after an authentication request has failed.

Use the **no** variant of this command to reset the quiet period to the default.

Syntax

```
auth timeout quiet-period <1-65535>
no auth timeout quiet-period
```

Parameter	Description
<1-65535>	Specifies the quiet period (in seconds).

Default The quiet period for port authentication is 60 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the quiet period to 10 seconds for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout quiet-period 10
```

To reset the quiet period to the default (60 seconds) for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout quiet-period
```

To set the quiet period to 10 seconds for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth timeout quiet-period 10
```

Related commands auth profile (global)

auth timeout reauth-period

Overview Use this command to set the timer for reauthentication on a given interface. The re-authentication for the supplicant (client device) is executed at this timeout. The timeout is only applied if the **auth reauthentication** command is applied.

Use the **no** variant of this command to reset the **reauth-period** parameter to the default (3600 seconds).

Syntax

```
auth timeout reauth-period <1-4294967295>
no auth timeout reauth-period
```

Parameter	Description
<1-4294967295>	The reauthentication timeout period (in seconds).

Default The default reauthentication period for port authentication is 3600 seconds, when reauthentication is enabled on the port.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the reauthentication period to 1 day for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout reauth-period 86400
```

To reset the reauthentication period to the default (3600 seconds) for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout reauth-period
```

To set the reauthentication period to 1 day for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth timeout reauth-period 86400
```

To reset the reauthentication period to the default (3600 seconds) for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth timeout reauth-period
```

Related commands

auth profile (global)

auth reauthentication

show dot1x

show dot1x interface

show running-config

auth timeout server-timeout

Overview Use this command to set the timeout for the waiting response from the RADIUS server on a given interface.

Use the **no** variant of this command to reset the server-timeout to the default (30 seconds).

Syntax

```
auth timeout server-timeout <1-65535>
no auth timeout server-timeout
```

Parameter	Description
<1-65535>	Server timeout period (in seconds).

Default The server timeout for port authentication is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the server timeout to 120 seconds for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout server-timeout 120
```

To set the server timeout to the default (30 seconds) for interface port1.0.2 use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout server-timeout
```

To set the server timeout to 120 seconds for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth timeout server-timeout 120
```

To set the server timeout to the default (30 seconds) for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth timeout server-timeout
```

Related commands auth profile (global)

show dot1x

show dot1x interface

show running-config

auth timeout supp-timeout

Overview This command sets the timeout of the waiting response from the supplicant (client device) on a given interface.

The **no** variant of this command resets the supplicant timeout to the default (30 seconds).

Syntax

```
auth timeout supp-timeout <1-65535>
no auth timeout supp-timeout
```

Parameter	Description
<1-65535>	The supplicant timeout period (in seconds).

Default The supplicant timeout for port authentication is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the supplicant timeout to 2 seconds for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout supp-timeout 2
```

To reset the supplicant timeout to the default (30 seconds) for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout supp-timeout
```

To set the supplicant timeout to 2 seconds for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth timeout supp-timeout 2
```

Related commands

auth profile (global)

show dot1x

show dot1x interface

show running-config

auth two-step enable

Overview Use this command to enable a two-step authentication feature on an interface. When this feature is enabled, the supplicant is authorized in a two-step process. If authentication succeeds, the supplicant becomes authenticated.

Use this command to apply the two-step authentication method based on 802.1X, MAC or web authentication.

Use the **no** variant of this command to disable the two-step authentication feature.

Syntax

```
auth two-step enable
no auth two-step enable
```

Default Two step authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage The single step authentication methods (either user or device authentication) have a potential security risk:

- an unauthorized user can access the network with an authorized device, or
- an authorized user can access the network with an unauthorized device.

Two-step authentication solves this problem by authenticating both the user and the device. The supplicant will only become authenticated if both these steps are successful. If the first authentication step fails, then the second step is not started.

Examples To enable the two step authentication feature, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth two-step enable
```

To disable the two step authentication feature, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth two-step enable
```

To enable MAC authentication followed by 802.1X authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

To enable MAC authentication followed by web authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

To enable 802.1X authentication followed by web authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

To enable the two step authentication feature for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth two-step enable
```

Related Commands auth profile (global)

auth two-step order

show auth two-step supplicant brief

show auth

show auth interface

show auth supplicant

show dot1x

show dot1x interface

show dot1x supplicant

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

auth two-step order

Overview Use this command to configure the order for two-step authentication. Two-step authentication and the relevant authentication methods must be enabled on the interface.

Use the **no** variant of this command to reset the authentication order to the default.

Syntax

```
auth two-step order auth-mac {dot1x|auth-web}
auth two-step order dot1x {auth-mac|auth-web}
no auth two-step order
```

Parameter	Description
`auth-mac`	MAC authentication
`dot1x`	802.1X authentication
`auth-web`	Web authentication

Default Order is determined by the authentication methods configured on the interface (see **Usage notes**).

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes The default authentication order depends on the combination of the authentication methods configured on the interface:

- If auth-mac is configured then auth-mac will be the first method.
- If auth-mac is **not** configured then dot1x will become the first method.
- If only two methods are configured then the remaining method becomes the second method.
- If all three methods are configured then the second method is chosen based on the packet type received (dot1x for an EAPOL packet and auth-web for an HTTP packet).

Examples

To set the two-step authentication order on port1.0.1 for 802.1X authentication and then MAC authentication, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth two-step enable
awplus(config-if)# auth two-step order dot1x auth-mac
```

To reset the two-step authentication order back to the default, which would be MAC authentication then 802.1X authentication if configured as above, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no auth two-step order
```

Related commands

auth two-step enable

auth-mac enable

auth-web enable

dot1x port-control

show auth interface

show auth supplicant

Command changes

Version 5.5.0-0.3: command added

auth-mac accounting

Overview Use this command to override the **default** RADIUS accounting method for MAC-based authentication on an interface by allowing you to apply a user-defined named list.

Use the **no** variant of this command to remove the named list from the interface and apply the **default** method.

Syntax

```
auth-mac accounting {default|<list-name>}
no auth-mac accounting
```

Parameter	Description
`default`	Apply the default accounting method list
<list-name>	Apply the user-defined named list

Default The **default** method list is applied to an interface by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To apply the named list 'vlan10_acct' on the vlan10 interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# auth-mac accounting vlan10_acct
```

To remove the named list from the vlan10 interface and set the accounting method back to **default**, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no auth-mac accounting
```

Related commands aaa accounting auth-mac

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

auth-mac authentication

Overview This command overrides the **default** MAC authentication method on an interface by allowing you to apply a user-defined named list.

Use the **no** variant of this command to remove the named list from the interface and apply the **default** method.

Syntax

```
auth-mac authentication {default|<list-name>}
no auth-mac authentication
```

Parameter	Description
`default`	Apply the default authentication method list
`<list-name>`	Apply a user-defined named list

Default The **default** method list is applied to an interface by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To apply the named list 'vlan10_auth' on the vlan10 interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# auth-mac authentication vlan10_auth
```

To remove the named list from the vlan10 interface and set the authentication method back to **default**, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no auth-mac authentication
```

Related commands aaa authentication auth-mac

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

auth-mac enable

Overview This command enables MAC authentication on the interface specified in the Interface command mode.

Use the **no** variant of this command to disable MAC authentication on an interface.

Syntax

```
auth-mac enable
no auth-mac enable
```

Default MAC-Authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes Enabling **spanning-tree edgeport** on ports after enabling MAC authentication avoids unnecessary re-authentication when the port state changes, which does not happen when spanning tree edgeport is enabled. Note that re-authentication is correct behavior without **spanning-tree edgeport** enabled.

Applying **switchport mode access** on ports is also good practice to set the ports to access mode with ingress filtering turned on, whenever ports for MAC authentication are in a VLAN.

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.

Examples To enable MAC authentication on interface port1.0.2 and enable spanning tree edgeport to avoid unnecessary re-authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac enable
awplus(config-if)# spanning-tree edgeport
awplus(config-if)# switchport mode access
```

To disable MAC authentication on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-mac enable
```

To enable MAC authentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-mac enable
```

Related commands

auth profile (global)

show auth

show auth interface

show running-config

Command changes

Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

auth-mac method

Overview This command sets the type of authentication method for MAC authentication that is used with RADIUS on the interface specified in the interface command mode.

The **no** variant of this command resets the authentication method used to the default method (PAP) as the RADIUS authentication method used by the MAC authentication.

Syntax

```
auth-mac method [eap-md5|pap]
no auth-mac method
```

Parameter	Description
eap-md5	Enable EAP-MD5 as the authentication method.
pap	Enable PAP as the authentication method.

Default The MAC authentication method is PAP.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the MAC authentication method to PAP on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac method pap
```

To set the MAC authentication method to the default on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-mac method
```

To set the MAC authentication method to EAP-MD5 on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-mac method eap-md5
```

Related commands auth profile (global)

show auth

show auth interface

show running-config

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

auth-mac password

Overview This command changes the password for MAC-based authentication.

Use the **no** variant of this command to return the password to its default.

Syntax

```
auth-mac [encrypted] password <password>
no auth-mac password
```

Parameter	Description
`auth-mac`	MAC-based authentication
`encrypted`	Specify an encrypted password
`password`	Configure the password
<password>	The new password. Passwords can be up to 64 characters in length and can contain any printable characters except: • ? • " (double quotes) • space

Default By default, the password is the MAC address of the supplicant.

Mode Global Configuration

Usage notes Changing the password increases the security of MAC-based authentication, because the default password is easy for an attacker to discover. This is particularly important if:

- some MAC-based supplicants on the network are intelligent devices, such as computers, and/or
- you are using two-step authentication (see the "Ensuring Authentication Methods Require Different Usernames and Passwords" section of the AAA and Port Authentication Feature_Overview_and_Configuration_Guide).

Examples To change the password to verySecurePassword, use the commands:

```
awplus# configure terminal
awplus(config)# auth-mac password verySecurePassword
```

Related commands auth two-step enable

show auth

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

auth-mac reauth-relearning

Overview This command sets the MAC address learning of the supplicant (client device) to re-learning for re-authentication on the interface specified in the interface command mode.

Use the **no** variant of this command to disable the auth-mac re-learning option.

Syntax

```
auth-mac reauth-relearning
no auth-mac reauth-relearning
```

Default Re-learning for port authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To enable the re-authentication re-learning feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac reauth-relearning
```

To disable the re-authentication re-learning feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-mac reauth-relearning
```

To enable the re-authentication re-learning feature on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-mac reauth-relearning
```

Related commands

auth profile (global)

show auth

show auth interface

show running-config

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

auth-mac static

Overview This command configures MAC authentication to use static entries in the FDB. Static entries persist in the FDB, even if there is no traffic flow from the supplicant.

When static FDB entries are configured, the auth roaming disconnected command is supported for MAC authentication. This command allows a supplicant to move to another authenticating interface without re-authentication.

Use the **no** variant of this command to revert to dynamic FDB entries.

Syntax

```
auth-mac static
no auth-mac static
```

Default By default MAC authentication supplicants are added to the FDB dynamically.

Mode Global Configuration

Example To configure MAC authentication to use static FDB entries, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-mac static
```

To configure MAC authentication to use dynamic FDB entries, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-mac static
```

Related commands auth roaming disconnected

show auth

show dot1x

Command changes Version 5.4.7-2.4: Command added

Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

auth-mac username

Overview Use this command to specify the format of the MAC address in the username and password field when a request for MAC-based authorization is sent to a RADIUS server.

Syntax

```
auth-mac username {ietf|unformatted} {lower-case|upper-case}
```

Parameter	Description
`ietf`	The MAC address includes a hyphen between each 2 bytes. (Example: xx-xx-xx-xx-xx-xx)
`unformatted`	The MAC address does not include hyphens. (Example: xxxxxxxxxxxx)
`lower-case`	The MAC address uses lower-case characters (a-f)
`upper-case`	The MAC address uses upper-case characters (A-F)

Default

```
auth-mac username ietf lower-case
```

Mode Global Configuration

Usage This command is provided to allow other vendors', AlliedWare, and AlliedWare Plus switches to share the same format on the RADIUS server.

Example To configure the format of the MAC address in the username and password field to be changed to IETF and upper-case, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-mac username ietf upper-case
```

Related commands auth-mac username

show running-config

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

auth-web accounting

Overview This command overrides the default RADIUS accounting method for web-based authentication on an interface by allowing you to apply a user-defined named list.

Use the **no** variant of this command to remove the named list from the interface and apply the default method.

Syntax

```
auth-web accounting {default|<list-name>}
no auth-web accounting
```

Parameter	Description
`default`	Apply the default accounting method list
`<list-name>`	Apply a named accounting method list

Default The **default** method list is applied to an interface by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To apply the named list 'vlan10_acct' on the vlan10 interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# auth-web accounting vlan10_acct
```

To remove the named list from the vlan10 interface and set the accounting method back to default, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no auth-web accounting
```

Related commands aaa accounting auth-web

auth-web authentication

Overview Use this command to override the default web-based authentication method on an interface by allowing you to apply a user-defined named list.

Use the **no** variant of this command to remove the named list from the interface and apply the default method.

Syntax

```
auth-web authentication {default|<list-name>}
no auth-web authentication
```

Parameter	Description
`default`	Apply the default authentication method list
`<list-name>`	Apply the user-defined named list

Default The **default** method list is applied to an interface by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To apply the named list 'vlan10_auth' on the vlan10 interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# auth-web authentication vlan10_auth
```

To remove the named list from the vlan10 interface and set the authentication method back to default, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no auth-web authentication
```

Related commands aaa authentication auth-web

auth-web enable

Overview Use this command to enable web-based authentication in Interface mode on the interface specified.

Use the **no** variant of this command to apply its default.

Syntax

```
auth-web enable
no auth-web enable
```

Default Web authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes Web-based authentication cannot be enabled if DHCP snooping is enabled by using the service dhcp-snooping command, and vice versa. You need to configure an IPv4 address for the VLAN interface on which web authentication is running.

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.

Examples To enable web authentication on static-channel-group 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface sa2
awplus(config-if)# auth-web enable
```

To disable web authentication on static-channel-group 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface sa2
awplus(config-if)# no auth-web enable
```

To enable web authentication on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-web enable
```

To disable web authentication on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-web enable
```

Related commands

auth profile (global)

show auth

show auth interface

show running-config

auth-web forward

Overview Use this command to enable the web authentication packet forwarding feature on the interface specified. This command also enables ARP forwarding, and adds forwarded packets to the **tcp** or **udp** port number specified.

Use the **no** variant of this command to disable the specified packet forwarding feature on the interface.

Syntax

```
auth-web forward [<ip-address>|<ip-address/prefix-length>]
{dns|tcp <1-65535>|udp <1-65535>}
```

or

```
auth-web forward {arp|dhcp|dns|tcp <1-65535>|udp <1-65535>}
```

The **no** variants of this command are:

```
no auth-web forward [<ip-address>|<ip-address/prefix-length>]
{dns|tcp <1-65535>|udp <1-65535>}
```

or

```
no auth-web forward {arp|dhcp|dns|tcp <1-65535>|udp <1-65535>}
```

Parameter	Description
<ip-address> *<ip-address/prefix-length>*	The IP address or subnet on which the web authentication is to be enabled.
`arp`	Enable forwarding of ARP.
`dhcp`	Enable forwarding of DHCP (67/udp).
`dns`	Enable forwarding of DNS (53/udp).
`tcp`	Enable forwarding of TCP specified port number.
`<1-65535>`	TCP Port number.
`udp`	Enable forwarding of UDP specified port number.
`<1-65535>`	UDP Port number.

Default Packet forwarding for port authentication is enabled by default for “arp”, “dhcp” and “dns”.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage notes For more information about the *<ip-address>* parameter, and an example, see the “auth-web forward” section in the Alliedware Plus Technical Tips and Tricks.

Examples To enable the ARP forwarding feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web forward arp
```

To add TCP forwarding port 137 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web forward tcp 137
```

To add the DNS Server IP address 192.168.1.10 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth-web forward 192.168.1.10 dns
```

To disable the ARP forwarding feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward arp
```

To delete TCP forwarding port 137 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward tcp 137
```

To delete all TCP forwarding on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward tcp
```

To enable the ARP forwarding feature on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-web forward arp
```

To add TCP forwarding port 137 on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-web forward tcp 137
```

To disable the ARP forwarding feature on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-web forward arp
```

To delete TCP forwarding port 137 on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-web forward tcp 137
```

To delete all TCP forwarding on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-web forward tcp
```

Related commands

auth profile (global)

show auth

show auth interface

auth-web idle-timeout enable

Overview Use this command to enable the idle-timeout for client of web authentication on the interface.

The **no** variant of this command to disable the idle-timeout for client of web authentication on the interface.

Syntax

```
auth-web idle-timeout enable
no auth-web idle-timeout enable
```

Default The idle-timeout is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To enable the idle-timeout on an interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config)# auth-web enable
awplus(config-if)# auth-web idle-timeout enable
```

To disable the idle-timeout on an interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth-web idle-timeout enable
```

Related commands auth-web enable

auth-web idle-timeout timeout

auth-web idle-timeout timeout

Overview Use this command to set the timeout value for web authentication client in seconds. The client will be unauthorized when it does not have any activity for a period that exceeds the timeout value.

The **no** variant of this command sets the timeout value to the default setting, 3600 seconds.

Syntax

```
auth-web idle-timeout timeout <420-86400>
no auth-web idle-timeout timeout
```

Parameter	Description
<420-86400>	Time in seconds.

Default The timeout is 3600 seconds by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To set 30 minutes as the idle-timeout, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# auth-web idle-timeout timeout 1800
```

To return the idle-timeout to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no auth-web idle-timeout timeout
```

Related commands auth-web enable

auth-web idle-timeout enable

auth-web max-auth-fail

Overview Use this command to set the number of authentication failures allowed before rejecting further authentication requests. When the supplicant (client device) fails more than the specified number of times, then login requests are refused during the quiet period.

Use the **no** variant of this command to reset the maximum number of authentication failures to the default.

Syntax

```
auth-web max-auth-fail <0-10>
no auth-web max-auth-fail
```

Parameter	Description
<0-10>	The maximum number of authentication failures allowed before login requests are refused.

Default The maximum number of authentication failures is set to 3.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the lock count to 5 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web max-auth-fail 5
```

To set the lock count to the default on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web max-auth-fail
```

To set the lock count to 5 on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-web max-auth-fail 5
```

To set the lock count to the default on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-web max-auth-fail
```

Related commands

auth profile (global)

auth timeout quiet-period

show auth

show auth interface

show running-config

auth-web method

Overview Use this command to set the web authentication access method that is used with RADIUS on the interface specified.

Use the **no** variant of this command to set the authentication method to PAP for the interface specified when web authentication is also used with the RADIUS authentication method.

Syntax

```
auth-web method {eap-md5|pap}
no auth-web method
```

Parameter	Description
`eap-md5`	Enable EAP-MD5 as the authentication method.
`pap`	Enable PAP as the authentication method.

Default The web authentication method is set to PAP by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To set the web authentication method to EAP-MD5 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web method eap-md5
```

To set the web authentication method to EAP-MD5 for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-web method eap-md5
```

Related commands

auth profile (global)

show auth

show auth interface

show running-config

auth-web-server blocking-mode

Overview Use this command to enable blocking mode for the Web-Authentication server. The blocking mode displays an authentication success or failure screen immediately from the response result from a RADIUS server.

Use the **no** variant of this command to disable blocking mode for the Web-Authentication server.

Syntax

```
auth-web-server blocking-mode
no auth-web-server blocking-mode
```

Default By default, blocking mode is disabled for the Web-Authentication server.

Mode Global Configuration

Example To enable blocking mode for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server blocking-mode
```

To disable blocking mode for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server blocking-mode
```

Related commands

auth-web-server redirect-delay-time

show auth-web-server

show running-config

auth-web-server dhcp ipaddress

Overview Use this command to assign an IP address and enable the DHCP service on the Web-Authentication server for supplicants (client devices).

Use the **no** variant of this command to remove an IP address and disable the DHCP service on the Web-Authentication server for supplicants.

Syntax

```
auth-web-server dhcp ipaddress <ip-address/prefix-length>
no auth-web-server dhcp ipaddress
```

Parameter	Description
<ip-addr/prefix-length>	The IPv4 address and prefix length assigned for the DHCP service on the Web-Authentication server for supplicants.

Default No IP address for the Web-Authentication server is set by default.

Mode Global Configuration

Usage notes See the AAA and Port Authentication Feature Overview and Configuration Guide for information about:

- using DHCP with web authentication, and
- restrictions regarding combinations of authentication enhancements working together

You cannot use the IPv4 address assigned to the device's interface as the Web-Authentication server address.

Examples To assign the IP address 10.0.0.1 to the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp ipaddress 10.0.0.1/8
```

To remove an IP address on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp ipaddress
```

Related commands auth-web-server dhcp lease

show auth-web-server

show running-config

auth-web-server dhcp lease

Overview Use this command to set the DHCP lease time for supplicants (client devices) using the DHCP service on the Web-Authentication server.

Use the **no** variant of this command to reset to the default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server.

Syntax

```
auth-web-server dhcp lease <20-60>
no auth-web-server dhcp lease
```

Parameter	Description
<20-60>	DHCP lease time for supplicants using the DHCP service on the Web-Authentication server in seconds.

Default The default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server is set to 30 seconds.

Mode Global Configuration

Usage notes See the AAA and Port Authentication Feature Overview and Configuration Guide for information about:

- using DHCP with web authentication, and
- restrictions regarding combinations of authentication enhancements working together

Examples To set the DHCP lease time to 1 minute for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp lease 60
```

To reset the DHCP lease time to the default setting (30 seconds) for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp lease
```

Validation Commands show running-config

Related commands show auth-web-server

auth-web-server dhcp ipaddress

auth-web-server dhcp-wpad-option

Overview This command sets the DHCP WPAD (Web Proxy Auto-Discovery) option for the Web-Authentication temporary DHCP service.

For more information and examples, see the "Web Auth Proxy" section in the Alliedware Plus Technical Tips and Tricks.

Use the **no** variant of this command to disable the DHCP WPAD function.

Syntax

```
auth-web-server dhcp wpad-option <url>
no auth-web-server dhcp wpad-option
```

Parameter	Description
<url>	URL to the server which gets a .pac file.

Default The Web-Authentication server DHCP WPAD option is not set.

Mode Global Configuration

Usage notes If the supplicant is configured to use WPAD, the supplicant's web browser will use TCP port 80 as usual. Therefore, the packet can be intercepted by Web-Authentication as normal, and the Web-Authentication Login page can be sent. However, after authentication, the browser does not know where to get the WPAD file and so cannot access external web pages. The WPAD file is usually named proxy.pac file and tells the browser what web proxy to use.

Use this command to tell the supplicant where it can get this file from. The switch itself can be specified as the source for this file, and it can deliver it to the supplicant on request.

Example To specify that the proxy.pac file is found on the server at 192.168.1.100, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp wpad-option
http://192.168.1.100/proxy/proxy.pac
```

Related commands show auth-web-server

auth-web-server host-name

Overview This command assigns a hostname to the web authentication server.

Use the **no** variant of this command to remove the hostname from the web authentication server.

Syntax

```
auth-web-server host-name <hostname>
no auth-web-server host-name
```

Parameter	Description
<hostname>	URL string of the hostname

Default The web authentication server has no hostname.

Mode Global Configuration

Usage notes When the web authentication server uses HTTPS protocol, the web browser will validate the certificate. If the certificate is invalid, the web page gives a warning message before displaying server content. However, the web page will not give warning message if the server has a hostname same as the one stored in the installed certificate.

Examples To set the auth.example.com as the hostname of the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server host-name auth.example.com
```

To remove hostname auth.example.com from the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server host-name
```

Related commands aaa authentication auth-web

auth-web enable

auth-web-server intercept-port

Overview This command specifies any additional TCP port numbers that the Web-Authentication server is to intercept.

Use the **no** variant of this command to stop intercepting the TCP port numbers.

Syntax

```
auth-web-server intercept-port {<1-65535>|any}
no auth-web-server intercept-port {<1-65535>|any}
```

Parameter	Description
<1-65535>	TCP port number.
`any`	Intercept all TCP packets

Default No additional TCP port numbers are intercepted by default.

Mode Global Configuration

Usage notes If this command is not specified, AlliedWare Plus Web-Authentication intercepts the supplicant's initial TCP port 80 connection to a web page and sends it the Web-Authentication Login page. However, if the supplicant is configured to use a web proxy, then it will usually be using TCP port 8080 (or another user configured port number). In this case Web-Authentication cannot intercept the connection.

To overcome this limitation you can use this command to tell the switch which additional port it should intercept, and then send the Web-Authentication Login page to the supplicant.

When the web authentication switch is in a guest network, the switch does not know the proxy server's port number in the supplicant's proxy setting. To overcome this limitation, you can use the **any** option in this command to intercept all TCP packets.

When you use this command in conjunction with a proxy server configured in the web browser, you must add the proxy server's network as a 'No Proxy' network. You can specify 'No Proxy' networks in the proxy settings in your web browser. For more information, see the "Web Auth Proxy" section in the Alliedware Plus Technical Tips and Tricks.

Example To additionally intercept port number 3128, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server intercept-port 3128
```

Related commands show auth-web-server

auth-web-server ipaddress

Overview This command sets the IP address for the Web-Authentication server.

Use the **no** variant of this command to delete the IP address for the Web-Authentication server.

You cannot use the IPv4 address assigned to the device's interface as the Web-Authentication server address.

Syntax

```
auth-web-server ipaddress <ip-address>
no auth-web-server ipaddress
```

Parameter	Description
<ip-address>	Web-Authentication server dotted decimal IP address in A.B.C.D format.

Default The Web-Authentication server address on the system is not set by default.

Mode Global Configuration

Examples To set the IP address `10.0.0.1` to the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ipaddress 10.0.0.1
```

To delete the IP address from the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ipaddress
```

Validation Commands

show auth

show auth-web-server

show running-config

auth-web-server page language

Overview Use this command to set the presentation language of Web authentication pages. Titles and subtitles of Web authentication pages will be set accordingly. Note that presently only English or Japanese are offered.

Use the **no** variant of this command to set the presentation language of Web authentication pages to its default (English).

Syntax

```
auth-web-server page language {english|japanese}
no auth-web-server page language
```

Parameter	Description
english	Web authentication pages are presented in English.
japanese	Web authentication pages are presented in Japanese.

Default Web authentication pages are presented in English by default.

Mode Global Configuration

Examples To set Japanese as the presentation language of Web authentication pages, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page language japanese
```

To set English as the presentation language of Web authentication pages, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page language english
```

To unset the presentation language of Web authentication pages and use English as the default presentation language, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page language
```

Related commands

auth-web-server page title

auth-web-server page sub-title

show auth-web-server page

auth-web-server login-url

Overview This command sets the web-authentication login page URL. This lets you replace the login page with your own page. See "Customising the Login Page" in the AAA and Port Authentication Feature Overview and Configuration Guide for details.

Use the **no** variant of this command to delete the URL.

Syntax

```
auth-web-server login-url <URL>
no auth-web-server login-url
```

Parameter	Description
<URL>	Set login page URL

Default The built-in login page is set by default.

Mode Global Configuration

Examples To set http://example.com/login.html as the login page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server login-url
http://example.com/login.html
```

To unset the login page URL, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server login-url
```

Related commands show running-config

auth-web-server page logo

Overview This command sets the type of logo that will be displayed on the web authentication page.

Use the **no** variant of this command to set the logo type to **auto**.

Note that if you need to customize the login page extensively, you can instead replace it with your own page. See "Customising the Login Page" in the AAA and Port Authentication Feature Overview and Configuration Guide.

Syntax

```
auth-web-server page logo {auto|default|hidden}
no auth-web-server page logo
```

Parameter	Description
`auto`	Display the custom logo if installed; otherwise display the default logo
`default`	Display the default logo
`hidden`	Hide the logo

Default Logo type is **auto** by default.

Mode Global Configuration

Examples To display the default logo with ignoring installed custom logo, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page logo default
```

To set back to the default logo type **auto**, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page logo
```

Validation Commands show auth-web-server page

auth-web-server page sub-title

Overview This command sets the custom sub-title on the web authentication page.

Use the **no** variant of this command to reset the sub-title to its default.

Note that if you need to customize the login page extensively, you can instead replace it with your own page. See "Customising the Login Page" in the AAA and Port Authentication Feature Overview and Configuration Guide.

Syntax

```
auth-web-server page sub-title {hidden|text <sub-title>}
no auth-web-server page sub-title
```

Parameter	Description
`hidden`	Hide the sub-title
`<sub-title>`	Text string of the sub-title

Default "Allied-Telesis" is displayed by default.

Mode Global Configuration

Examples To set the custom sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title text Web
Authentication
```

To hide the sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title hidden
```

To change back to the default title, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page sub-title
```

Validation Commands show auth-web-server page

auth-web-server page success-message

Overview This command sets the success message on the web-authentication page.

Use the **no** variant of this command to remove the success message.

Note that if you need to customize the login page extensively, you can instead replace it with your own page. See "Customising the Login Page" in the AAA and Port Authentication Feature Overview and Configuration Guide.

Syntax

```
auth-web-server page success-message text <success-message>
no auth-web-server page success-message
```

Parameter	Description
<success-message>	Text string of the success message

Default No success message is set by default.

Mode Global Configuration

Examples To set the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page success-message text Your success message
```

To unset the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page success-message
```

Validation Commands show auth-web-server page

auth-web-server page title

Overview This command sets the custom title on the web authentication page.

Use the **no** variant of this command to remove the custom title.

Note that if you need to customize the login page extensively, you can instead replace it with your own page. See "Customising the Login Page" in the AAA and Port Authentication Feature Overview and Configuration Guide.

Syntax

```
auth-web-server page title {hidden|text <title>}
no auth-web-server page title
```

Parameter	Description
`hidden`	Hide the title
`<title>`	Text string of the title

Default "Web Access Authentication Gateway" is displayed by default.

Mode Global Configuration

Examples To set the custom title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page title text Login
```

To hide the title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page title hidden
```

To unset the custom title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page title
```

Validation Commands show auth-web-server page

auth-web-server page welcome-message

Overview This command sets the welcome message on the web-authentication login page.

Use the **no** variant of this command to remove the welcome message.

Note that if you need to customize the login page extensively, you can instead replace it with your own page. See "Customising the Login Page" in the AAA and Port Authentication Feature Overview and Configuration Guide.

Syntax

```
auth-web-server page welcome-message text <welcome-message>
no auth-web-server page welcome-message
```

Parameter	Description
<welcome-message>	Text string of the welcome message

Default No welcome message is set by default.

Mode Global Configuration

Examples To set the welcome message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page welcome-message text Your welcome message
```

To remove the welcome message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page welcome-message
```

Validation Commands show auth-web-server page

auth-web-server ping-poll enable

Overview This command enables the ping polling to the supplicant (client device) that is authenticated by Web-Authentication.

The **no** variant of this command disables the ping polling to the supplicant that is authenticated by Web-Authentication.

Syntax

```
auth-web-server ping-poll enable
no auth-web-server ping-poll enable
```

Default The ping polling feature for Web-Authentication is disabled by default.

Mode Global Configuration

Examples To enable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll enable
```

To disable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll enable
```

Validation Commands

show auth

show auth-web-server

show running-config

auth-web-server ping-poll failcount

Overview This command sets a fail count for the ping polling feature when used with Web-Authentication. The **failcount** parameter specifies the number of unanswered pings. A supplicant (client device) is logged off when the number of unanswered pings are greater than the failcount set with this command.

Use the **no** variant of this command to resets the fail count for the ping polling feature to the default (5 pings).

Syntax

```
auth-web-server ping-poll failcount <1-100>
no auth-web-server ping-poll failcount
```

Parameter	Description
<1-100>	Count.

Default The default failcount for ping polling is 5 pings.

Mode Global Configuration

Examples To set the failcount of ping polling to `10` pings, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll failcount 10
```

To set the failcount of ping polling to default, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll failcount
```

Validation Commands show auth

show auth-web-server

show running-config

auth-web-server ping-poll interval

Overview This command is used to change the ping poll interval. The interval specifies the time period between pings when the supplicant (client device) is reachable.

Use the **no** variant of this command to reset to the default period for ping polling (30 seconds).

Syntax

```
auth-web-server ping-poll interval <1-65535>
no auth-web-server ping-poll interval
```

Parameter	Description
<1-65535>	Seconds.

Default The interval for ping polling is 30 seconds by default.

Mode Global Configuration

Examples To set the interval of ping polling to `60` seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll interval 60
```

To set the interval of ping polling to the default (30 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll interval
```

Validation Commands

show auth

show auth-web-server

show running-config

auth-web-server ping-poll reauth-timer-refresh

Overview This command modifies the **reauth-timer-refresh** parameter for the Web-Authentication feature. The **reauth-timer-refresh** parameter specifies whether a re-authentication timer is reset and when the response from a supplicant (a client device) is received.

Use the **no** variant of this command to reset the **reauth-timer-refresh** parameter to the default setting (disabled).

Syntax

```
auth-web-server ping-poll reauth-timer-refresh
no auth-web-server ping-poll reauth-timer-refresh
```

Default The `reauth-timer-refresh` parameter is disabled by default.

Mode Global Configuration

Examples To enable the `reauth-timer-refresh` timer, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll reauth-timer-refresh
```

To disable the `reauth-timer-refresh` timer, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll
reauth-timer-refresh
```

Validation Commands show auth

show auth-web-server

show running-config

auth-web-server ping-poll timeout

Overview This command modifies the ping poll **timeout** parameter for the Web-Authentication feature. The **timeout** parameter specifies the time in seconds to wait for a response to a ping packet.

Use the **no** variant of this command to reset the timeout of ping polling to the default (1 second).

Syntax

```
auth-web-server ping-poll timeout <1-30>
no auth-web-server ping-poll timeout
```

Parameter	Description
<1-30>	Seconds.

Default The default timeout for ping polling is 1 second.

Mode Global Configuration

Examples To set the timeout of ping polling to 2 seconds, use the command:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll timeout 2
```

To set the timeout of ping polling to the default (1 second), use the command:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll timeout
```

Validation Commands

show auth

show auth-web-server

show running-config

auth-web-server port

Overview This command sets the HTTP port number for the Web-Authentication server.

Use the **no** variant of this command to reset the HTTP port number to the default (80).

Syntax

```
auth-web-server port <port-number>
no auth-web-server port
```

Parameter	Description
<port-number>	Set the local Web-Authentication server port within the TCP port number range 1 to 65535.

Default The Web-Authentication server HTTP port number is set to 80 by default.

Mode Global Configuration

Examples To set the HTTP port number `8080` for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server port 8080
```

To reset to the default HTTP port number `80` for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server port
```

Validation Commands show auth

show auth-web-server

show running-config

auth-web-server redirect-delay-time

Overview Use this command to set the delay time in seconds before redirecting the supplicant to a specified URL when the supplicant is authorized.

Use the variant **no** to reset the delay time set previously.

Syntax

```
auth-web-server redirect-delay-time <5-60>
no auth-web-server redirect-delay-time
```

Parameter	Description
`redirect-delay-time`	Set the delay time before jumping to a specified URL after the supplicant is authorized.
<5-60>	The time in seconds.

Default The default redirect delay time is `5` seconds.

Mode Global Configuration

Examples To set the delay time to `60` seconds for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-delay-time 60
```

To reset the delay time, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-delay-time
```

Related commands

auth-web-server blocking-mode

auth-web-server redirect-url

show auth-web-server

show running-config

auth-web-server redirect-url

Overview This command sets a URL for supplicant (client device) authentication. When a supplicant is authorized it will be automatically redirected to the specified URL. Note that if the http redirect feature is used then this command is ignored.

Use the **no** variant of this command to delete the URL string set previously.

Syntax

```
auth-web-server redirect-url <url>
no auth-web-server redirect-url
```

Parameter	Description
<url>	URL (hostname or dotted IP notation).

Default The redirect URL for the Web-Authentication server feature is not set by default (null).

Mode Global Configuration

Examples To enable and set redirect a URL string www.alliedtelesis.com for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-url
http://www.alliedtelesis.com
```

To delete a redirect URL string, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-url
```

Related commands

auth-web-server redirect-delay-time

show auth

show auth-web-server

show running-config

auth-web-server session-keep

Overview This command enables the session-keep feature to jump to the original URL after being authorized by Web-Authentication.

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

Syntax
```
auth-web-server session-keep
no auth-web-server session-keep
```

Default The session-keep feature is disabled by default.

Mode Global Configuration

Usage notes This function doesn't ensure to keep session information in all cases. Authenticated supplicant may be redirected to unexpected page when session-keep is enabled. This issue occurred by supplicant sending HTTP packets automatically after authentication page is displayed and the URL is written.

Examples To enable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server session-keep
```

To disable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server session-keep
```

Validation Commands

show auth

show auth-web-server

show running-config

auth-web-server ssl

Overview This command enables HTTPS functionality for the Web-Authentication server feature.

Use the **no** variant of this command to disable HTTPS functionality for the Web-Authentication server.

Syntax

```
auth-web-server ssl
no auth-web-server ssl
```

Default HTTPS functionality for the Web-Authentication server feature is disabled by default.

Mode Global Configuration

Examples To enable HTTPS functionality for the Web-Authentication server feature, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ssl
```

To disable HTTPS functionality for the Web-Authentication server feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ssl
```

Validation Commands show auth

show auth-web-server

show running-config

auth-web-server ssl intercept-port

Overview Use this command to register HTTPS intercept port numbers when the HTTPS server uses custom port number (not TCP port number 443).

Note that you need to use the **auth-web-server intercept-port** command to register HTTP intercept port numbers.

Use the **no** variant of this command to delete registered port number.

Syntax

```
auth-web-server ssl intercept-port <1-65535>
no auth-web-server ssl intercept-port <1-65535>
```

Parameter	Description
<1-65535>	TCP port number in the range from 1 through 65535

Default 443/TCP is registered by default.

Mode Global Configuration

Examples To register HTTPS port number 3128, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ssl intercept-port 3128
```

To delete HTTPS port number 3128, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ssl intercept-port 3128
```

Validation Commands show auth-web-server

Related commands auth-web-server intercept-port

copy proxy-autoconfig-file

Overview Use this command to download the proxy auto configuration (PAC) file to your switch. The Web-Authentication supplicant can get the downloaded file from the system web server.

Syntax

```
copy <filename> proxy-autoconfig-file
```

Parameter	Description
<filename>	The URL of the PAC file.

Mode Privileged Exec

Example To download the PAC file to this device, use the command:

```
awplus# copy tftp://server/proxy.pac proxy-autoconfig-file
```

Related commands

show proxy-autoconfig-file

erase proxy-autoconfig-file

copy web-auth-https-file

Overview Use this command to download the SSL server certificate for web-based authentication. The file must be in PEM (Privacy Enhanced Mail) format, and contain the private key and the server certificate.

Syntax

```
copy <filename> web-auth-https-file
```

Parameter	Description
<filename>	The URL of the server certificate file.

Mode Privileged Exec

Example To download the server certificate file `veriSign_cert.pem` from the TFTP server directory `server`, use the command:

```
awplus# copy tftp://server/veriSign_cert.pem
web-auth-https-file
```

Related commands

auth-web-server ssl

erase web-auth-https-file

show auth-web-server

description (auth-profile)

Overview Use this command to add a description to an authentication profile in Authentication Profile mode.

Use the **no** variant of this command to remove the current description.

Syntax

```
description <description>
```

Parameter	Description
<description>	Text describing the selected authentication profile.

Default No description configured by default.

Mode Authentication Profile

Example To add a description to the authentication profile 'student', use the following commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# description student room setting
```

To remove a description from the authentication profile 'student', use the following commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no description
```

Related commands auth profile (global)

erase proxy-autoconfig-file

Overview Use this command to remove the proxy auto configuration file.

Syntax

```
erase proxy-autoconfig-file
```

Mode Privileged Exec

Example To remove the proxy auto configuration file, use the command:

```
awplus# erase proxy-autoconfig-file
```

Related commands

show proxy-autoconfig-file

copy proxy-autoconfig-file

erase web-auth-https-file

Overview Use this command to remove the SSL server certificate for web-based authentication.

Syntax

```
erase web-auth-https-file
```

Mode Privileged Exec

Example To remove the SSL server certificate file for web-based authentication use the command:

```
awplus# erase web-auth-https-file
```

Related commands

auth-web-server ssl

copy web-auth-https-file

show auth-web-server

platform l3-vlan-hashing-algorithm

Overview This command enables you to change the L3 VLAN hash-key-generating algorithm.

The **no** variant of this command returns the hash-key algorithm to the default of crc32l.

Syntax

```
platform l3-vlan-hashing-algorithm
{crc16l|crc16u|crc32l|crc32u}
```

```
no platform l3-vlan-hashing-algorithm
```

Parameter	Description
`crc16l`	The algorithm that will apply to the lower bits of CRC-16
`crc16u`	The algorithm that will apply to the upper bits of CRC-16
`crc32l`	The algorithm that will apply to the lower bits of CRC-32
`crc32u`	The algorithm that will apply to the upper bits of CRC-32

Default The hash-key algorithm is crc32l by default.

Mode Global configuration

Usage notes Occasionally, when using the Multiple Dynamic VLAN feature, a supplicant cannot be authenticated because a collision occurs within the VLAN L3 table. This can happen when more than four different IP addresses produce the same hash-key.

When this situation occurs, collisions can sometimes be avoided by changing the hashing algorithm from its default of crc32l. Several different algorithms may need to be tried to rectify the problem.

You must restart the switch for this command to take effect.

Note that this command is intended for technical support staff, or advanced end users.

Example To change the hash-key generating algorithm applying to the lower bits of CRC-16, use the command:

```
awplus# configure terminal
awplus(config)# platform l3-vlan-hashing-algorithm crc16l
```

Related commands platform mac-vlan-hashing-algorithm

show platform

platform mac-vlan-hashing-algorithm

Overview This command enables you to change the MAC VLAN hash-key-generating algorithm.

The **no** variant of this command returns the hash-key algorithm to the default of crc32l

Syntax

```
platform mac-vlan-hashing-algorithm
{crc16l|crc16u|crc32l|crc32u}
```

```
no platform mac-vlan-hashing-algorithm
```

Parameter	Description
`crc16l`	The algorithm that will apply to the lower bits of CRC-16
`crc16u`	The algorithm that will apply to the upper bits of CRC-16
`crc32l`	The algorithm that will apply to the lower bits of CRC-32
`crc32u`	The algorithm that will apply to the upper bits of CRC-32

Default The hash-key algorithm is crc32l by default.

Mode Global configuration

Usage notes Occasionally, when using the Multiple Dynamic VLAN feature, a supplicant cannot be authenticated because a collision occurs within the VLAN MAC table. This can happen when more than four different MAC addresses produce the same hash-key.

When this situation occurs, collisions can sometimes be avoided by changing the hashing algorithm from its default of crc32l. Several different algorithms may need to be tried to rectify the problem.

You must restart the switch for this command to take effect.

Note that this command is intended for technical support staff, or advanced end users.

Example To change the hash-key generating algorithm applying to the lower bits of CRC-16, use the command:

```
awplus# configure terminal
awplus(config)# platform mac-vlan-hashing-algorithm crc16l
```

Related commands platform l3-vlan-hashing-algorithm

show platform

show auth

Overview This command shows the configuration state of authentication.

Syntax

```
show auth [all]
```

Parameter	Description
`all`	Display all authentication information for each authenticated interface. This can be a static channel (or static aggregator), or a dynamic (or LACP) channel group, or a switch port.

Mode Privileged Exec

Example To display all authentication information, enter the command:

```
awplus# show auth all
```

Output Figure 44-1: Example output from the **show auth** command

```
awplus# show auth all
802.1X Port-Based Authentication Enabled
MAC-based Port Authentication Disabled
WEB-based Port Authentication Enabled
 RADIUS server address (auth): 150.87.17.192:1812
   Last radius message id: 4
Authentication Info for interface port1.0.1
 portEnabled: true - portControl: Auto
 portStatus: Authorized
 reAuthenticate: disabled
 reAuthPeriod: 3600
 PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
 BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in
 KT: keyTxEnabled: false
 critical: disabled
 guestVlan: disabled
 authFailVlan: disabled
 dynamicVlanCreation: disabled
 multiVlanCreation: disabled
 hostMode: single-host
 dot1x: enabled
   protocolVersion: 1
 authMac: disabled
 authWeb: enabled
   method: PAP
   maxAuthFail: 3
   packetForwarding:
     10.0.0.1 80/tcp
     dns
     dhcp
```

```
twoStepAuthentication:
   configured: enabled
   actual: enabled
supplicantMac: none
Supplicant name: oha
Supplicant address: 000d.6013.5398
   authenticationMethod: WEB-based Authentication
   Two-Step Authentication:
     firstAuthentication: Pass - Method: dot1x
     secondAuthentication: Pass - Method: web
   portStatus: Authorized - currentId: 3
   abort:F fail:F start:F timeout:F success:T
   PAE: state: Authenticated - portMode: Auto
   PAE: reAuthCount: 0 - rxRespId: 0
   PAE: quietPeriod: 60 - maxReauthReq: 2
   BE: state: Idle - reqCount: 0 - idFromServer: 2
   CD: adminControlledDirections: in - operControlledDirections: in
   CD: bridgeDetected: false
   KR: rxKey: false
   KT: keyAvailable: false - keyTxEnabled: false
```

Related commands show dot1x

show auth diagnostics

Overview This command shows authentication diagnostics, optionally for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

Syntax

```
show auth diagnostics [interface <interface-list>]
```

Parameter	Description
`interface`	Specify ports to show.
`<interface-list>`	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example To display authentication diagnostics for port1.0.6, enter the command:

```
awplus# show auth diagnostics interface port1.0.6
```

Output Figure 44-2: Example output from the **show auth diagnostics** command

```
Authentication Diagnostics for interface port1.0.6
     Supplicant address: 00d0.59ab.7037
         authEnterConnecting: 2
         authEaplogoffWhileConnecting: 1
         authEnterAuthenticating: 2
         authSuccessWhileAuthenticating: 1
         authTimeoutWhileAuthenticating: 1
         authFailWhileAuthenticating: 0
         authEapstartWhileAuthenticating: 0
         authEaplogoggWhileAuthenticating: 0
         authReauthsWhileAuthenticated: 0
         authEapstartWhileAuthenticated: 0
      authEaplogoffWhileAuthenticated: 0
         BackendResponses: 2
         BackendAccessChallenges: 1
         BackendOtherrequestToSupplicant: 3
         BackendAuthSuccess: 1
```

Related commands show dot1x interface

show auth interface

Overview This command shows the status of port authentication on the specified interface.

Syntax

```
show auth interface <interface-list>
```

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • a continuous range of interfaces separated by a hyphen (e.g. port1.0.1-port1.0.3) • a comma-separated list (e.g. port1.0.1, port1.0.3-port1.0.4). Do not mix interface types in a list.

Mode Privileged Exec

Example To display the web-based authentication status for port1.0.4, enter the command:

```
awplus# show auth interface port1.0.4
```

If port-based authentication is not configured, the output will be

```
% Port-Control not configured on port1.0.4
```

To display the port-based authentication status for port1.0.4, enter the command:

```
awplus# show auth interface port1.0.4
```

```
awplus# show auth interface port1.0.4
Authentication Info for interface port1.0.4
 portEnabled: true - portControl: Auto
 portStatus: Authorized
 reAuthenticate: disabled
 reAuthPeriod: 3600
 PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
 BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in
 KT: keyTxEnabled: false
 critical: disabled
 guestVlan: disabled
 guestVlanForwarding:none
 authFailVlan: disabled
 dynamicVlanCreation: disabled
 multiVlanCreation: disabled
 hostMode: single-host
 dot1x: enabled
   protocolVersion: 1
 authMac: disabled
 authWeb: enabled
   method: PAP
   maxAuthFail: 3
   packetForwarding:
     10.0.0.1 80/tcp
     dns
     dhcp
 twoStepAuthentication:
   configured: enabled
   actual: enabled
   order: dot1x auth-web
 supplicantMac: none
```

Related commands

show auth diagnostics

show dot1x sessionstatistics

show dot1x statistics interface

show dot1x supplicant interface

show auth sessionstatistics

Overview This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Syntax

```
show auth sessionstatistics [interface <interface-list>]
```

Parameter	Description
`interface`	Specify ports to show.
`<interface-list>`	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example To display authentication statistics for port1.0.6, enter the command:

```
awplus# show auth sessionstatistics interface port1.0.6
```

Output Figure 44-3: Example output from the **show auth sessionstatistics** command

```
Authentication session statistics for interface port1.0.6
     session user name: manager
         session authentication method: Remote server
         session time: 19440 secs
         session terminat cause: Not terminated yet
```

show auth statistics interface

Overview Use this command to show the authentication statistics for the specified interface.

Syntax

```
show auth statistics interface <interface-list>
```

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • a continuous range of interfaces separated by a hyphen (e.g. port1.0.1-port1.0.3) • a comma-separated list (e.g. port1.0.1, port1.0.3-port1.0.4). Do not mix interface types in a list.

Mode Privileged Exec

Example To display authentication statistics for port1.0.2, enter the command:

```
awplus# show auth statistics interface port1.0.2
```

Output Figure 44-4: Example output from **show auth statistics interface** for a port

```
awplus# show auth statistics interface port1.0.2
802.1X statistics for interface port1.0.2
   EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
   EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
   EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
 EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
   Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
   EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame
Src:00d0.59ab.7037
```

Related commands show dot1x interface

show auth supplicant

Overview Use this command to show the supplicant (client device) state when authentication is configured for the switch. Use the optional **brief** parameter to show a summary of the supplicant state.

Syntax

```
show auth supplicant [<macadd>] [brief]
```

Parameter	Description
<macadd>	Mac (hardware) address of the supplicant. Entry format is HHHH.HHHH.HHHH (hexadecimal).
`brief`	Brief summary of the supplicant state.

Mode Privileged Exec

Examples To display a summary of authenticated supplicant information on the device, enter the command:

```
awplus# show auth supplicant brief
```

To display authenticated supplicant information on the device, enter the command:

```
awplus# show auth supplicant
```

To display authenticated supplicant information for the device with MAC address 0000.5E00.5301, enter the command:

```
awplus# show auth supplicant 0000.5E00.5301
```

Output Figure 44-5: Example output from **show auth supplicant brief**

```
awplus#show auth supplicant brief
Interface port1.0.3
  authenticationMethod: dot1x/mac/web
  Two-Step Authentication
    firstMethod: mac
    secondMethod: dot1x/web
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 0
    webBasedAuthenticationSupplicantNum: 1
    otherAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address    Status            IP Address      Username
=========== ==== ==== ============== ================= =============== ========
port1.0.3   1    W    001c.233e.e15a Authenticated     192.168.1.181   test
port1.0.3   1    D    0240.4040.4040 Authenticated     --              test
port1.0.3   1    Q    0230.3030.3030 Authenticated     192.168.1.181   test
```

Figure 44-6: Example output from **show auth supplicant**

```
awplus#show auth supplicant
Interface port1.0.3
  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: 0000.5E00.5301
    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
    dynamicVlanId: 999
    dynamicTaggedVlanId: 0
    RADIUS server group (auth): radius
    RADIUS server (auth): 192.168.1.40
    Session timeout enabled: No
    dynamicACL Rules:
      ip:deny ip 10.37.165.10/24 any
      ip:permit ip any any
      ipv6:deny ipv6 any any
    Quarantined: true
    Quarantine Vlan: 999
```

Figure 44-7: Example output from **show auth supplicant 0000.5E00.5301**

```
awplus#show auth supplicant 0000.5E00.5301
Interface port1.0.3
  Supplicant name: test
  Supplicant address: 0000.5E00.5301
    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
    Quarantined: true
    Quarantine Vlan: 999
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    RADIUS server group (auth): radius
    RADIUS server (auth): 192.168.1.40
    Session timeout enabled: No
    dynamicACL Rules:
      ip:deny ip 10.37.165.10/24 any
      ip:permit ip any any
      ipv6:deny ipv6 any any
```

Related commands

aaa accounting auth-mac

aaa accounting auth-web

aaa accounting dot1x

aaa authentication auth-mac

aaa authentication auth-web

aaa authentication dot1x

show auth supplicant interface

Overview This command shows the supplicant (client device) state for the authentication mode set for the interface. Use the optional **brief** parameter to show a summary of the supplicant state.

Syntax

```
show auth-web supplicant interface <interface-list> [brief]
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`brief`	Brief summary of the supplicant state.

Mode Privileged Exec

Examples To display the authenticated supplicant on the interface port1.0.2, enter the command:

```
awplus# show auth supplicant interface port1.0.2
```

To display brief summary output for the authenticated supplicant on the interface port1.0.2, enter the command:

```
awplus# show auth supplicant interface port1.0.2 brief
```

show auth two-step supplicant brief

Overview This command displays the supplicant state of the two-step authentication feature on the interface.

Syntax

```
show auth two-step supplicant [interface <interface-list>]
brief
```

Parameter	Description
`interface`	The interface selected for display.
<interface-list>	The interfaces to display information about. An interface-list can be: • a VLAN (e.g. vlan2) • a switchport (e.g. port1.0.4) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • a continuous range of interfaces separated by a hyphen (e.g. port1.0.1-port1.0.3) • a comma-separated list (e.g. port1.0.1, port1.0.3-port1.0.4). Do not mix interface types in a list.

Mode Privileged Exec

Usage notes Do not mix interface types in a list. The specified interfaces must exist.

Example To display the supplicant state of the two-step authentication feature, enter the command:

```
awplus# show two-step supplicant interface port1.0.2 brief
```

Output Figure 44-8: Example output from **show auth two-step supplicant brief**

```
interface port1.0.2

  authenticationMethod: dot1x/mac

  Two-Step Authentication:
    firstMethod:mac
    secondMethod:dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    webBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0

Interface  VID Mode  MAC Address       Status          FirstStep     SecondStep
========== === ====  ===========       ======          =========     ==========
port1.0.8  1   D     000b..db67.00f7   Authenticated   Pass          Pass
```

Related commands auth two-step enable

Command changes Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

show auth-web-server

Overview This command shows the Web-Authentication server configuration and status on the switch.

Syntax

```
show auth-web-server
```

Mode Privileged Exec

Example To display Web-Authentication server configuration and status, enter the command:

```
awplus# show auth-web-server
```

Output Figure 44-9: Example output from the **show auth-web-server** command

```
Web authentication server
     Server status: enabled
     Server mode: none
     Server address: 192.168.1.1/24
       DHCP server enabled
       DHCP lease time: 20
       DHCP WPAD Option URL: http://192.168.1.1/proxy.pac
     HTTP Port No: 80
     Security: disabled
     Certification: default
     SSL Port No: 443
     Redirect URL: --
     Redirect Delay Time: 5
     HTTP Redirect: enabled
     Session keep: disabled
     PingPolling: disabled
     PingInterval: 30
     Timeout: 1
     FailCount: 5
     ReauthTimerReFresh: disabled
```

Related commands

auth-web-server ipaddress

auth-web-server port

auth-web-server redirect-delay-time

auth-web-server redirect-url

auth-web-server session-keep

auth-web-server ssl

show auth-web-server page

Overview This command displays the web-authentication page configuration and status.

Syntax

```
show auth-web-server page
```

Mode Privileged Exec

Examples To show the web-authentication page information, use the command:

```
awplus# show auth-web-server page
```

Figure 44-10: Example output from the **show auth-web-server page** command

```
awplus#show auth-web-server page
Web authentication page
  Logo: auto
  Title: default
  Sub-Title: Web Authentication
  Welcome message: Your welcome message
  Success message: Your success message
```

Related commands

auth-web forward

auth-web-server page logo

auth-web-server page sub-title

auth-web-server page success-message

auth-web-server page title

auth-web-server page welcome-message

show proxy-autoconfig-file

Overview This command displays the contents of the proxy auto configuration (PAC) file.

Syntax

```
show proxy-autoconfig-file
```

Mode Privileged Exec

Example To display the contents of the proxy auto configuration (PAC) file, enter the command:

```
awplus# show auth proxy-autoconfig-file
```

Output Figure 44-11: Example output from **show proxy-autoconfig-file**

```
function FindProxyForURL(url,host)
{
 if (isPlainHostName(host) ||
     isInNet(host, "192.168.1.0","255.255.255.0")) {
   return "DIRECT";
}
 else {
   return "PROXY 192.168.110.1:8080";
 }
}
```

Related commands

copy proxy-autoconfig-file

erase proxy-autoconfig-file

45 AAA Commands

Introduction

Overview

AAA is the collective title for the three related functions of Authentication, Authorization and Accounting. These function 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 auth-mac" on page 2285
- "aaa accounting auth-web" on page 2287
- "aaa accounting commands" on page 2289
- "aaa accounting dot1x" on page 2291
- "aaa accounting login" on page 2293
- "aaa accounting update" on page 2296
- "aaa authentication auth-mac" on page 2298
- "aaa authentication auth-web" on page 2300
- "aaa authentication dot1x" on page 2302
- "aaa authentication enable default group tacacs+" on page 2304
- "aaa authentication enable default local" on page 2306

- "aaa authentication login" on page 2307
- "aaa authorization commands" on page 2309
- "aaa authorization config-commands" on page 2311
- "aaa group server" on page 2312
- "aaa local authentication attempts lockout-time" on page 2314
- "aaa local authentication attempts max-fail" on page 2315
- "aaa login fail-delay" on page 2316
- "accounting login" on page 2317
- "authorization commands" on page 2318
- "clear aaa local user lockout" on page 2320
- "debug aaa" on page 2321
- "login authentication" on page 2322
- "proxy-port" on page 2323
- "radius-secure-proxy aaa" on page 2324
- "server (radsecproxy-aaa)" on page 2325
- "server mutual-authentication" on page 2327
- "server name-check" on page 2328
- "server trustpoint" on page 2329
- "show aaa local user locked" on page 2331
- "show aaa server group" on page 2332
- "show debugging aaa" on page 2333
- "show radius server group" on page 2334
- "undebug aaa" on page 2336

aaa accounting auth-mac

Overview This command configures an accounting method list for MAC-based authentication. An accounting method list specifies what type of accounting messages are sent and which RADIUS servers the accounting messages are sent to. Use this command to configure either the default method list, which is automatically applied to interfaces with MAC-based authentication enabled, or a named method list, which can be applied to an interface with the auth-mac accounting command.

Use the **no** variant of this command to disable either the default or a named accounting method list for MAC-based authentication. Once all method lists are disabled, AAA accounting for MAC-based authentication is disabled globally.

Syntax
```
aaa accounting auth-mac {default|<list-name>}
{start-stop|stop-only|none} group {<group-name>|radius}
no aaa accounting auth-mac {default|<list-name>}
```

Parameter	Description
`default`	Configure the default accounting method list
`<list-name>`	Configure a named accounting method list
`start-stop`	Sends a start accounting message at the beginning of the session and a stop accounting message at the end of the session.
`stop-only`	Only sends a stop accounting message at the end of the session.
`none`	No accounting record sent.
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default RADIUS accounting for MAC-based Authentication is disabled by default

Mode Global Configuration

Usage notes This command can be used to configure either the default accounting method list or a named accounting method list:

- **default**: the default accounting method list which is automatically applied to all interfaces with MAC-based authentication enabled.
- *<list-name>*: a user named list which can be applied to an interface using the auth-mac accounting command.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by radius-server host command

- **group** <*group-name*>: use the specified RADIUS server group configured with the aaa group server command

The accounting event to send to the RADIUS server is configured with the following options:

- **start-stop**: sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only**: sends a **stop** accounting message at the end of a session.
- **none**: disables accounting.

Examples To enable the default RADIUS accounting for MAC-based authentication, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-mac default start-stop
group radius
```

To disable RADIUS accounting for MAC-based Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-mac default
```

To enable a named RADIUS accounting method list 'vlan10_acct' for MAC-based authentication, with the RADIUS server group 'rad_group_vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-mac vlan10_acct start-stop
group rad_group_vlan10
```

To disable a named RADIUS accounting method list 'vlan10_acct' for MAC-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-mac vlan10_acct
```

Related commands

aaa authentication auth-mac

aaa group server

auth-mac accounting

auth-mac enable

radius-server host

show aaa server group

aaa accounting auth-web

Overview This command configures an accounting method list for Web-based authentication. An accounting method list specifies what type of accounting messages are sent and which RADIUS servers the accounting messages are sent to. Use this command to configure either the default method list, which is automatically applied to interfaces with Web-based authentication enabled, or a named method list, which can be applied to an interface with the auth-web accounting command.

Use the **no** variant of this command to disable either the default or a named accounting method list for Web-based authentication. Once all method lists are disabled, AAA accounting for Web-based authentication is disabled globally.

Syntax

```
aaa accounting auth-web {default|<list-name>}
{start-stop|stop-only|none} group {<group-name>|radius}
```

```
no aaa accounting auth-web {default|<list-name>}
```

Parameter	Description
`default`	Configure the default accounting method list
`<list-name>`	Configure a named accounting method list
`start-stop`	Sends a start accounting message at the beginning of the session and a stop accounting message at the end of the session.
`stop-only`	Only sends a stop accounting message at the end of the session.
`none`	No accounting record sent.
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default RADIUS accounting for Web-based authentication is disabled by default.

Mode Global Configuration

Usage notes This command can be used to configure either the default accounting method list or a named accounting method list:

- **default**: the default accounting method list which is automatically applied to all interfaces with Web-based authentication enabled.
- *<list-name>*: a user named list which can be applied to an interface using the auth-web accounting command.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by radius-server host command

- **group** <*group-name*>: use the specified RADIUS server group configured with the aaa group server command

Configure the accounting event to be sent to the RADIUS server with the following options:

- **start-stop**: sends a start accounting message at the beginning of a session and a stop accounting message at the end of the session.
- **stop-only**: sends a stop accounting message at the end of a session.
- **none**: disables accounting.

Examples To enable the default RADIUS accounting method for Web-based authentication, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-web default start-stop
group radius
```

To disable the default RADIUS accounting method for Web-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-web default
```

To enable a named RADIUS accounting method list 'vlan10_acct' for Web-based authentication, with the RADIUS server group 'rad_group_vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-web vlan10_acct start-stop
group rad_group_vlan10
```

To disable a named RADIUS accounting method list 'vlan10_acct' for Web-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-web vlan10_acct
```

Related commands

aaa authentication auth-web

aaa group server

auth-web accounting

auth-web enable

radius-server host

show aaa server group

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.

TACACS+ is not available in Secure Mode (see the crypto secure-mode command).

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 dot1x

Overview Use this command to configure an accounting method list for IEEE 802.1X-based authentication. An accounting method list specifies what type of accounting messages are sent and which RADIUS servers the accounting messages are sent to. Use this command to configure either the default method list, which is automatically applied to interfaces with IEEE 802.1X-based authentication enabled, or a named method list, which can be applied to an interface with the dot1x accounting command.

Use the **no** variant of this command to disable either the default or a named accounting method list for 802.1X-based authentication. Once all method lists are disabled, AAA accounting for 802.1x-based authentication is disabled globally.

Syntax

```
aaa accounting dot1x {default|<list-name>}
{start-stop|stop-only|none} group {<group-name>|radius}

no aaa accounting dot1x {default|<list-name>}
```

Parameter	Description
`default`	Configure the default accounting method list
`<list-name>`	Configure a named accounting method list
`start-stop`	Sends a start accounting message at the beginning of the session and a stop accounting message at the end of the session.
`stop-only`	Only sends a stop accounting message at the end of the session.
`none`	No accounting record sent.
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default RADIUS accounting for 802.1X-based authentication is disabled by default (there is no default server set by default).

Mode Global Configuration

Usage notes This command can be used to configure either the default accounting method list or a named accounting method list:

- **default**: the default accounting method list which is automatically applied to all interfaces with 802.1X-based authentication enabled.
- *<list-name>*: a user named list which can be applied to an interface using the dot1x accounting command.

There are two ways to define servers where RADIUS accounting messages will be sent:

- **group radius**: use all RADIUS servers configured by radius-server host command.
- **group** <*group-name*>: use the specified RADIUS server group configured with the aaa group server command.

The accounting event to send to the RADIUS server is configured by the following options:

- **start-stop**: sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only**: sends a **stop** accounting message at the end of a session.
- **none**: disables accounting.

Examples

To enable RADIUS accounting for 802.1X-based authentication, and use all available RADIUS Servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting dot1x default start-stop group radius
```

To disable RADIUS accounting for 802.1X-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting dot1x default
```

To enable a named RADIUS accounting method list 'vlan10_acct' for 802.1X-based authentication, with the RADIUS server group 'rad_group_vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting dot1x vlan10_acct start-stop group rad_group_vlan10
```

To disable a named RADIUS accounting method list 'vlan10_acct' for 802.1X-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting dot1x vlan10_acct
```

Related commands

aaa accounting update

aaa authentication dot1x

aaa group server

dot1x accounting

dot1x port-control

radius-server host

show aaa server group

Command changes

Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

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.

TACACS+ is not available in Secure Mode (see the crypto secure-mode command).

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

aaa accounting update

accounting login

radius-server host

tacacs-server host

aaa accounting update

Overview This command enables periodic accounting reporting to either the RADIUS or TACACS+ accounting server(s) wherever login accounting has been configured.

Note that unlimited RADIUS servers and up to four TACACS+ servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the **no** variant of this command to disable periodic accounting reporting to the accounting server(s).

Syntax

```
aaa accounting update [periodic <1-65535>]
no aaa accounting update
```

Parameter	Description
`periodic`	Send accounting records periodically.
<1-65535>	The interval to send accounting updates (in minutes). The default is 30 minutes.

Default Periodic accounting update is disabled by default.

Mode Global Configuration

Usage notes Use this command to enable the device to send periodic AAA login accounting reports to the accounting server. When periodic accounting report is enabled, interim accounting records are sent according to the interval specified by the **periodic** parameter. The accounting updates are start messages.

If the **no** variant of this command is used to disable periodic accounting reporting, any interval specified by the **periodic** parameter is reset to the default of 30 minutes when accounting reporting is reenabled, unless this interval is specified.

Examples To configure the switch to send period accounting updates every 30 minutes, the default period, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update
```

To configure the switch to send period accounting updates every 10 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update periodic 10
```

To disable periodic accounting update wherever accounting has been configured, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting update
```

Related commands

aaa accounting auth-mac

aaa accounting auth-web

aaa accounting dot1x

aaa accounting login

aaa authentication auth-mac

Overview This command enables MAC-based authentication globally and allows you to enable either the default authentication method list (in this case, a list of RADIUS servers), which is automatically applied to every interface running MAC-based authentication, or a user named authentication method list, which is applied to an interface with the auth-mac authentication command.

Use the **no** variant of this command to disable either the default or a named method list for MAC-based authentication. Once all method lists are disabled MAC-based authentication is disabled globally.

Syntax

```
aaa authentication auth-mac {default|<list-name>} group
{<group-name>|radius}
```

```
no aaa authentication auth-mac {default|<list-name>}
```

Parameter	Description
`default`	Configure the default authentication method list
`<list-name>`	Configure a named authentication method list
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default MAC-based Port Authentication is disabled by default.

Mode Global Configuration

Usage notes This command can be used to configure either the default authentication method list or a named authentication method list:

- **default**: the default authentication method list which is automatically applied to all interfaces with Web-based authentication enabled.
- **<***list-name***>**: a user named list which can be applied to an interface using the auth-web authentication command.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by radius-server host command
- **group** <*group-name*>: use the specified RADIUS server group configured with the aaa group server command

All configured RADIUS Servers are automatically members of the server group **radius**. If a server is added to a named group <*group-name*>, it also remains a member of the group **radius**.

Examples

To enable MAC-based authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-mac default group radius
```

To disable MAC-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-mac default
```

To enable MAC-based authentication for named list 'vlan10_auth', with RADIUS server group 'rad_group_vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-mac vlan10_auth group rad_group_vlan10
```

To disable MAC-based authentication for named list 'vlan10_auth', use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-mac vlan10_acct
```

Related commands

aaa accounting auth-mac

aaa group server

auth-mac authentication

auth-mac enable

radius-server host

show aaa server group

aaa authentication auth-web

Overview This command enables Web-based authentication globally and allows you to enable either the default authentication method list (in this case, a list of RADIUS servers), which is automatically applied to every interface running Web-based authentication, or a user named authentication method list, which is applied to an interface with the auth-web authentication command.

Use the **no** variant of this command to disable either the default or a named method list for Web-based authentication. Once all method lists are disabled Web-based authentication is disabled globally.

Syntax

```
aaa authentication auth-web {default|<list-name>} group
{<group-name>|radius}
```

```
no aaa authentication auth-web {default|<list-name>}
```

Parameter	Description
`default`	Configure the default authentication method list
`<list-name>`	Configure a named authentication method list
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default Web-based authentication is disabled by default.

Mode Global Configuration

Usage notes This command can be used to configure either the default authentication method list or a named authentication method list:

- **default**: the default authentication method list which is automatically applied to all interfaces with Web-based authentication enabled.
- **<***list-name***>**: a user named list which can be applied to an interface using the auth-web authentication command.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by radius-server host command
- **group <***group-name***>**: use the specified RADIUS server group configured with the aaa group server command

Note that you need to configure an IPv4 address for the VLAN interface on which Web authentication is running.

Examples

To enable Web-based authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-web default group radius
```

To disable Web-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-web default
```

To enable Web-based authentication for named list 'vlan10_auth', with RADIUS server group 'rad_group_vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-web vlan10_auth group rad_group_vlan10
```

To disable Web-based authentication for named list 'vlan10_auth', use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication vlan10_auth
```

Related commands

aaa accounting auth-web

aaa group server

auth-web authentication

auth-web enable

radius-server host

aaa authentication dot1x

Overview Use this command to enable IEEE 802.1X-based authentication globally and to allow you to enable either the default authentication method list (in this case, a list of RADIUS servers), which is automatically applied to every interface running IEEE 802.1X-based authentication, or a user named authentication method list, which is applied to an interface with the dot1x authentication command.

Use the **no** variant of this command to disable either the default or a named method list for 802.1X-based authentication. Once all method lists are disabled 802.1x-based authentication is disabled globally.

Syntax

```
aaa authentication dot1x {default|<list-name>} group
{<group-name>|radius}
```

```
no aaa authentication dot1x {default|<list-name>}
```

Parameter	Description
`default`	Configure the default authentication method list
`<list-name>`	Configure a named authentication method list
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default 802.1X-based Port Authentication is disabled by default.

Mode Global Configuration

Usage notes This command can be used to configure either the default authentication method list or a named authentication method list:

- **default**: the default authentication method list which is automatically applied to all interfaces with 802.1X-based authentication enabled.
- *<list-name>*: a user named list which can be applied to an interface using the aaa authentication dot1x command.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by radius-server host command
- **group** *<group-name>*: use the specified RADIUS server group configured with the aaa group server command

Examples To enable 802.1X-based authentication globally with all RADIUS servers, and use all available RADIUS servers, use the command:

```
awplus# configure terminal
```

```
awplus(config)# aaa authentication dot1x default group radius
```

To disable 802.1X-based authentication, use the command:

```
awplus# configure terminal
awplus(config)# no aaa authentication dot1x default
```

To enable 802.1X-based authentication for named list 'vlan10_auth', with RADIUS server group 'rad_group_vlan10', use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication dot1x vlan10_auth group
rad_group_vlan10
```

To disable 802.1X-based authentication for named list 'vlan10_auth' use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication dot1x vlan10_acct
```

Related commands

aaa accounting dot1x

aaa group server

dot1x authentication

dot1x port-control

radius-server host

show aaa server group

Command changes

Version 5.4.9-2.1: command added to AR2050V, AR3050S, and AR4050S

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.

TACACS+ is not available in Secure Mode (see the crypto secure-mode command).

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 to use to authenticate user login, or to replace an existing method list with the same name. Specify one or more of the options **local** or **group**, in the order you want them to be applied. If the **default** method list name is specified, it is applied to every console and VTY line immediately unless another method list is applied to that line by the login authentication command. To apply a non-default method list, you must also use the login authentication command.

TACACS+ is not available in Secure Mode (see the crypto secure-mode command).

Use the **no** variant of this command to remove an authentication method list for user login. The specified method list name is deleted from the configuration. If the method list name has been applied to any console or VTY line, user login authentication on that line will fail.

Note that the **no aaa authentication login default** command does not remove the default method list. This will return the default method list to its default state (**local** is the default).

Syntax

```
aaa authentication login {default|<list-name>} {[local] [group
{radius|tacacs+|<group-name>}]}
no aaa authentication login {default|<list-name>}
```

Parameter	Description
`default`	Set the default authentication server for user login.
`<list-name>`	Name of authentication server.
`local`	Use the local username database.
`group`	Use server group.
`radius`	Use all RADIUS servers configured by the 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 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 **loginauthentication** command.

local is the default state for the default method list unless a named method list is applied to that line by the **login authentication** command. Reset to the default method list using the **no aaa authentication login default** command.

Mode Global Configuration

Usage 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 not the local user database; the user login fails.

Examples To configure the default authentication method list for user login to first use all available RADIUS servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login default group radius
local
```

To configure a user login authentication method list called **USERS** to first use the RADIUS server group `RAD_GROUP1` for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group RAD_GROUP1
local
```

To configure a user login authentication method list called USERS to first use the TACACS+ servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group tacacs+
local
```

To return to the default method list (**local** is the default server), use the following commands:

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

To delete an existing authentication method list USERS created for user login authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication login USERS
```

Related commands aaa accounting commands

aaa authentication enable default group tacacs+

login authentication

aaa 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 This command configures a RADIUS server group. A server group can be used to specify a subset of RADIUS servers in **aaa** commands. The group name **radius** is predefined, which includes all RADIUS servers configured by the **radius-server host** command.

RADIUS servers are added to a server group using the **server** command. Each RADIUS server should be configured using the **radius-server host** command.

Use the **no** variant of this command to remove an existing RADIUS server group.

Syntax

```
aaa group server radius <group-name>
no aaa group server radius <group-name>
```

Parameter	Description
<group-name>	Server group name.

Mode Global Configuration

Usage notes Use this command to create an AAA group of RADIUS servers, and to enter Server Group Configuration mode, in which you can add servers to the group. Use a server group to specify a subset of RADIUS servers in AAA commands. Each RADIUS server must be configured by the **radius-server host** command. To add RADIUS servers to a server group, use the **server** command.

Examples To create a RADIUS server group named `GROUP1` with hosts `192.168.1.1`, `192.168.2.1` and `192.168.3.1`, use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.2.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.3.1 auth-port 1812 acct-port 1813
```

To remove a RADIUS server group named `GROUP1` from the configuration, use the command:

```
awplus(config)# no aaa group server radius GROUP1
```

Related commands

aaa accounting auth-mac

aaa accounting auth-web

aaa accounting dot1x

aaa accounting login

aaa authentication auth-mac

aaa authentication auth-web

aaa authentication dot1x

aaa authentication login

radius-server host

server (server group)

show radius server group

aaa local authentication attempts lockout-time

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

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

Syntax

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

Parameter	Description
<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

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

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

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 current number of failed attempts, last failure time and location against each user account attempting to log into the device.

Note that once the lockout count has been manually cleared by another privileged account using the clear aaa local user lockout command or a locked account successfully logs into the system after waiting for the lockout time, this command will display nothing for that particular account.

Syntax

```
show aaa local user locked
```

Mode User Exec and Privileged Exec

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

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

Output Figure 45-1: Example output from the **show aaa local user locked** command

```
awplus# show aaa local user locked
Login           Failures Latest failure     From
bob                  3    05/23/14 16:21:37  ttyS0
manager              5    05/23/14 16:31:44  192.168.1.200
```

Related commands

aaa local authentication attempts lockout-time

aaa local authentication attempts max-fail

clear aaa local user lockout

show 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 45-2: 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 -             -                -       -
-------- ---- ------------- ---------------- ------- ----------
dot1x    auth default       radius           group   -
-------- ---- ------------- ---------------- ------- ----------
dot1x    acct vlan30_acct   rad_group_4      group   start-stop
-------- ---- ------------- ---------------- ------- ----------
auth-mac auth default       radius           group   -
-------- ---- ------------- ---------------- ------- ----------
auth-mac acct vlan10_acct   rad_group_vlan10 group   start-stop
-------- ---- ------------- ---------------- ------- ----------
auth-web auth default       radius           group   -
-------- ---- ------------- ---------------- ------- ----------
auth-web acct default       rad_group_3      group   start-stop
-------- ---- ------------- ---------------- ------- ----------
openvpn  auth -             -                -       -
-------- ---- ------------- ---------------- ------- ----------
isakmp   auth default       radius           group   -
-------- ---- ------------- ---------------- ------- ----------
```

Related commands

aaa accounting auth-mac

aaa accounting auth-web

aaa accounting dot1x

aaa accounting auth-mac

aaa authentication auth-web

aaa authentication dot1x

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 45-3: 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 45-4: 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 45-5: 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.

46 RADIUS Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure the device to use RADIUS servers. For more information, see the RADIUS Feature Overview and Configuration Guide.

Command List

- "auth radius send nas-identifier" on page 2338
- "auth radius send service-type" on page 2339
- "deadtime (RADIUS server group)" on page 2340
- "debug radius" on page 2341
- "ip radius source-interface" on page 2342
- "radius-server deadtime" on page 2343
- "radius-server host" on page 2344
- "radius-server key" on page 2348
- "radius-server retransmit" on page 2350
- "radius-server timeout" on page 2352
- "server (server group)" on page 2354
- "show debugging radius" on page 2356
- "show radius" on page 2357
- "show radius statistics" on page 2360
- "undebug radius" on page 2361

auth radius send nas-identifier

Overview Use this command to enable the device to include the NAS-Identifier(32) attribute in RADIUS authentication requests.

Use the **no** variant of this command to stop including the NAS-Identifier attribute.

Syntax

```
auth radius send nas-identifier [<name>|vlan-id]
no auth radius send nas-identifier
```

Parameter	Description
<name>	Send this user-defined text as the NAS-Identifier. You can specify up to 253 characters.
vlan-id	Send the VLAN ID of the authentication port as the NAS-Identifier. This is the configured VLAN ID, not the dynamic VLAN ID or guest VLAN ID.

Mode Global Configuration

Example To use a user-defined identifier of NASID100 as the NAS-Identifier attribute, use the commands:

```
awplus# configure terminal
awplus(config)# auth radius send nas-identifier NASID100
```

To use the VLAN ID as the NAS-Identifier attribute, use the commands:

```
awplus# configure terminal
awplus(config)# auth radius send nas-identifier vlan-id
```

To stop sending the NAS-Identifier attribute, use the commands:

```
awplus# configure terminal
awplus(config)# no auth radius send nas-identifier
```

Related commands auth radius send service-type

auth radius send service-type

Overview Use this command to enable the device to include the Service-Type(6) attribute in RADIUS authentication requests. The Service-Type attribute has a value of:

- Framed(2) for 802.1x
- Call-Check(10) for MAC authentication
- Unbound(5) for Web authentication.

Use the **no** variant of this command to stop including the Service-Type attribute.

Syntax

```
auth radius send service-type
no auth radius send service-type
```

Mode Global Configuration

Example To send the Service-Type attribute, use the commands:

```
awplus# configure terminal
awplus(config)# auth radius send service-type
```

Related commands auth radius send nas-identifier

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 Server Group Configuration

Usage If the RADIUS server does not respond to a request packet, the packet is retransmitted the number of times configured for the **retransmit** parameter (after waiting for a **timeout** period to expire). The server is then marked "dead", and the time is recorded. The **deadtime** parameter configures the amount of time to skip a dead server; if a server is dead, no request message is sent to the server for the **deadtime** period.

Examples To configure the deadtime for 5 minutes for the RADIUS server group "GROUP1", use the command:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1
awplus(config-sg)# deadtime 5
```

To remove the deadtime configured for the RADIUS server group "GROUP1", use the command:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no deadtime
```

Related commands aaa group server

radius-server deadtime

debug radius

Overview This command enables RADIUS debugging. If no option is specified, all debugging options are enabled.

Use the **no** variant of this command to disable RADIUS debugging. If no option is specified, all debugging options are disabled.

Syntax

```
debug radius [packet|event|all]
no debug radius [packet|event|all]
```

Parameter	Description
`packet`	Debugging for RADIUS packets is enabled or disabled.
`event`	Debugging for RADIUS events is enabled or disabled.
`all`	Enable or disable all debugging options.

Default RADIUS debugging is disabled by default.

Mode Privileged Exec

Examples To enable debugging for RADIUS packets, use the command:

```
awplus#  debug radius packet
```

To enable debugging for RADIUS events, use the command:

```
awplus#  debug radius event
```

To disable debugging for RADIUS packets, use the command:

```
awplus# no debug radius packet
```

To disable debugging for RADIUS events, use the command:

```
awplus# no debug radius event
```

Related commands show debugging radius

undebug radius

ip radius source-interface

Overview This command configures the source IP address of every outgoing RADIUS packet to use a specific IP address or the IP address of a specific interface. If the specified interface is down or there is no IP address on the interface, then the source IP address of outgoing RADIUS packets depends on the interface the packets leave.

Use the **no** variant of this command to remove the source interface configuration. The source IP address in outgoing RADIUS packets will be the IP address of the interface from which the packets are sent.

Syntax

```
ip radius source-interface {<interface>|<ip-address>}
no ip radius source-interface
```

Parameter	Description
<interface>	Interface name.
<ip-address>	IP address in the dotted decimal format A.B.C.D.

Default Source IP address of outgoing RADIUS packets depends on the interface the packets leave.

Mode Global Configuration

Examples To configure all outgoing RADIUS packets to use the IP address of the interface “vlan1” for the source IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface vlan1
```

To configure the source IP address of all outgoing RADIUS packets to use 192.168.1.10, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface 192.168.1.10
```

To reset the source interface configuration for all outgoing RADIUS packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip radius source-interface
```

Related commands radius-server host

show radius statistics

radius-server deadtime

Overview Use this command to specify the global **deadtime** for all RADIUS servers. If a RADIUS server is considered dead, it is skipped for the specified deadtime. This command specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

Use the **no** variant of this command to reset the global deadtime to the default of 0 seconds, so that RADIUS servers are not skipped even if they are dead.

Syntax

```
radius-server deadtime <minutes>
no radius-server deadtime
```

Parameter	Description
<minutes>	RADIUS server deadtime in minutes in the range 0 to 1440 (24 hours).

Default The default RADIUS deadtime configured on the system is 0 seconds.

Mode Global Configuration

Usage The RADIUS client considers a RADIUS server to be dead if it fails to respond to a request after it has been retransmitted as often as specified globally by the radius-server retransmit command or for the server by the radius-server host command. To improve RADIUS response times when some servers may be unavailable, set a **deadtime** to skip dead servers.

Examples To set the dead time of the RADIUS server to 60 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server deadtime 60
```

To disable the dead time of the RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server deadtime
```

Related commands

deadtime (RADIUS server group)

radius-server host

radius-server retransmit

show radius statistics

radius-server host

Overview Use this command to specify a remote RADIUS server host for authentication or accounting, and to set server-specific parameters. The parameters specified with this command override the corresponding global parameters for RADIUS servers. This command specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination UDP port numbers.

This command adds the RADIUS server address and sets parameters to the RADIUS server. The RADIUS server is added to the running configuration after you issue this command. If parameters are not set using this command then common system settings are applied.

Use the **no** variant of this command to remove the specified server host as a RADIUS authentication and/or accounting server and set the destination port to the default RADIUS server port number (1812).

Syntax

```
radius-server host {<host-name>|<ip-address>} [acct-port
<0-65535>] [auth-port <0-65535>] [key <key-string>] [retransmit
<0-100>] [timeout <1-1000>]
```

```
radius-server host {<host-name>|<ip-address>} [acct-port
<0-65535>] [auth-port <0-65535>] [key-encrypted
<encrypted-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.
`key-encrypted`	Set an encrypted shared secret key. When secure mode is enabled, the running configuration contains this parameter instead of the key parameter. It indicates that the device stores keys in the running configuration in encrypted form instead of in plain text.
<encrypted-key -string>	Encrypted shared key string.

Default The RADIUS client address is not configured (null) by default. No RADIUS server is configured.

Mode Global Configuration

Usage Multiple **radius -server host** commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified. If no host-specific timeout, retransmit, or key values are specified, the global values apply to that host. If there are multiple RADIUS servers for this client, use this command multiple times—once to specify each server.

If you specify a host without specifying the auth port or the acct port, it will by default be configured for both authentication and accounting, using the default UDP ports. To set a host to be a RADIUS server for authentication requests only, set

the **acct-port** parameter to 0; to set the host to be a RADIUS server for accounting requests only, set the auth-port parameter to 0.

A RADIUS server is identified by IP address, authentication port and accounting port. A single host can be configured multiple times with different authentication or accounting ports. All the RADIUS servers configured with this command are included in the predefined RADIUS server group radius, which may be used by AAA authentication, authorization and accounting commands. The client transmits (and retransmits, according to the **retransmit** and **timeout** parameters) RADIUS authentication or accounting requests to the servers in the order you specify them, until it gets a response.

Examples To add the RADIUS server `10.0.0.20`, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20
```

To set the secret key to **allied** on the RADIUS server `10.0.0.20`, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 key allied
```

To delete the RADIUS server `10.0.0.20`, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host 10.0.0.20
```

To configure `rad1.company.com` for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad1.company.com acct-port 0
```

To remove the RADIUS server `rad1.company.com` configured for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host rad1.company.com
acct-port 0
```

To configure `rad2.company.com` for accounting only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad2.company.com auth-port 0
```

To configure 192.168.1.1 with authentication port 1000, accounting port 1001 and retransmit count 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 192.168.1.1 auth-port 1000
acct-port 1001 retransmit 5
```

Command changes Version 5.4.9-2.1: **key-encrypted** parameter added.

Related commands

aaa group server

radius-server key

radius-server retransmit

radius-server timeout

show radius statistics

radius-server key

Overview This command sets a global secret key for RADIUS authentication on the device. The shared secret text string is used for RADIUS authentication between the device and a RADIUS server.

Note that if no secret key is explicitly specified for a RADIUS server, the global secret key will be used for the shared secret for the server.

Use the **no** variant of this command to reset the secret key to the default (null).

Syntax

```
radius-server key <key-string>
no radius-server key
```

When in secure mode, the syntax in config files will be:

```
radius-server key-encrypted <encrypted-key-string>
```

Parameter	Description
`key <key-string>`	Shared secret among RADIUS server and 802.1X client.
`key-encrypted <encrypted-key-string>`	This parameter indicates that the key is in its encrypted form. You would not normally enter this command. Instead, if you enter key and secure mode is enabled, the running config contains this parameter instead of the key parameter. This indicates that in secure mode the device stores keys in the running config in encrypted form instead of in plain text.

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

show radius statistics

radius-server retransmit

Overview This command sets the retransmit counter to use RADIUS authentication on the device. This command specifies how many times the device transmits each RADIUS request to the RADIUS server before giving up.

This command configures the **retransmit** parameter for RADIUS servers globally. If the **retransmit** parameter is not specified for a RADIUS server by the **radius-server host** command then the global configuration set by this command is used for the server instead.

Use the **no** variant of this command to reset the re-transmit counter to the default (3).

Syntax

```
radius-server retransmit <retries>
no radius-server retransmit
```

Parameter	Description
<retries>	RADIUS server retries in the range <0-100>. The number of times a request is resent to a RADIUS server that does not respond, before the server is considered dead and the next server is tried. If no retransmit value is specified for a particular RADIUS server using the **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

show radius statistics

radius-server timeout

Overview Use this command to specify the RADIUS global timeout value. This is how long the device waits for a reply to a RADIUS request before retransmitting the request, or considering the server to be dead. If no timeout is specified for the particular RADIUS server by the **radius-server host** command, it uses this global timeout value.

Note that this command configures the **timeout** parameter for RADIUS servers globally.

The **no** variant of this command resets the transmit timeout to the default (5 seconds).

Syntax

```
radius-server timeout <seconds>
no radius-server timeout
```

Parameter	Description
<seconds>	RADIUS server timeout in seconds in the range 1 to 1000. The global time in seconds to wait for a RADIUS server to reply to a request before retransmitting the request, or considering the server to be dead (depending on the **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

show radius statistics

server (server group)

Overview This command adds a RADIUS server to a server group in Server-Group Configuration mode. The RADIUS server should be configured by the radius-server host command.

The server is appended to the server list of the group and the order of configuration determines the precedence of servers. If the server exists in the server group already, it will be removed before added as a new server.

The server is identified by IP address and authentication and accounting UDP port numbers. So a RADIUS server can have multiple entries in a group with different authentication and/or accounting UDP ports. The **auth-port** specifies the UDP destination port for authentication requests to the server. To disable authentication for the server, set `auth-port` to 0. If the authentication port is missing, the default port number is 1812. The **acct-port** specifies the UDP destination port for accounting requests to the server. To disable accounting for the server, set `acct-port` to 0. If the accounting port is missing, the default port number is 1812.

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 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 auth-mac

aaa accounting auth-web

aaa accounting dot1x

aaa accounting login

aaa authentication auth-mac

aaa authentication auth-web

aaa authentication login

aaa group server

radius-server host

show debugging radius

Overview This command displays the current debugging status for the RADIUS servers.

Syntax

```
show debugging radius
```

Mode User Exec and Privileged Exec

Example To display the current debugging status of RADIUS servers, use the command:

```
awplus# show debugging radius
```

Output Figure 46-1: 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 46-2: 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 46-3: 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 statistics

Overview This command shows the RADIUS client statistics for the device.

Syntax

```
show radius statistics
```

Mode User Exec and Privileged Exec

Example See the sample output below showing RADIUS client statistics and RADIUS configuration:

```
awplus# show radius statistics
```

Output Figure 46-4: Example output from the **show radius statistics** command:

```
RADIUS statistics for Server: 150.87.18.89
 Access-Request Tx  : 5 - Retransmit  : 0
 Access-Accept Rx  : 1 - Access-Reject Rx  : 2
 Access-Challenge Rx  : 2
 Unknown Type  : 0 - Bad Authenticator : 0
 Malformed Access-Resp : 0 - Wrong Identifier : 0
 Bad Attribute  : 0 - Packet Dropped  : 0
 TimeOut  : 0 - Dead count  : 0
 Pending Request : 0
```

undebug radius

Overview This command applies the functionality of the **no** debug radius command.

47 Local RADIUS Server Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure the local RADIUS server on the device. For more information, see the Local RADIUS Server Feature Overview and Configuration Guide.

The local RADIUS server is not available in Secure Mode (see the crypto secure-mode command.

Command List

- "attribute" on page 2364
- "authentication" on page 2366
- "client (radsecproxy-srv)" on page 2367
- "client mutual-authentication" on page 2369
- "client name-check" on page 2370
- "client trustpoint" on page 2371
- "clear radius local-server statistics" on page 2372
- "copy fdb-radius-users (to file)" on page 2373
- "copy local-radius-user-db (from file)" on page 2375
- "copy local-radius-user-db (to file)" on page 2376
- "crypto pki enroll local (deleted)" on page 2377
- "crypto pki enroll local local-radius-all-users (deleted)" on page 2378
- "crypto pki enroll local user (deleted)" on page 2379
- "crypto pki export local pem (deleted)" on page 2380
- "crypto pki export local pkcs12 (deleted)" on page 2381
- "crypto pki trustpoint local (deleted)" on page 2382
- "debug crypto pki (deleted)" on page 2383
- "domain-style" on page 2384

- "egress-vlan-id" on page 2385
- "egress-vlan-name" on page 2387
- "group" on page 2389
- "nas" on page 2390
- "help radius-attribute" on page 2391
- "radius-secure-proxy local-server" on page 2393
- "radius-server local" on page 2394
- "server auth-port" on page 2395
- "server enable" on page 2396
- "show radius local-server group" on page 2397
- "show radius local-server nas" on page 2398
- "show radius local-server statistics" on page 2399
- "show radius local-server user" on page 2400
- "user (RADIUS server)" on page 2402
- "vlan (RADIUS server)" on page 2404

attribute

Overview Use this command to define a RADIUS attribute for the local RADIUS server user group.

For a complete list of defined RADIUS attributes and values, see the Local RADIUS Server Feature Overview and Configuration Guide.

When used with the **value** parameter the **attribute** command configures RADIUS attributes to the user group. If the specified attribute is already defined then it is replaced with the new value.

Use the **no** variant of this command to delete an attribute from the local RADIUS server user group.

Syntax

```
attribute [repeated] {<attribute-name>|<attribute-id>} <value>
no attribute {<attribute-name>|<attribute-id>}
```

Parameter	Description
`repeated`	This optional parameter allows you to set multiple instances of the same attribute name or attribute id.
<attribute-name>	RADIUS attribute name for standard attributes or Vendor-Specific attributes (see the Local RADIUS Server Feature Overview and Configuration Guide for tables of attributes).
<attribute-id>	RADIUS attribute numeric identifier for standard attributes.
<value>	RADIUS attribute value.

Default By default, no attributes are configured.

Mode RADIUS Server Group Configuration

Usage notes For the Standard attributes, the attribute may be specified using either the attribute name, or its numeric identifier. For example, the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause 1
```

will produce the same results as the command:

```
awplus(config-radsrv-group)# attribute 49 1
```

In the same way, where the specific attribute has a pre-defined value, the parameter *<value>* may be substituted with the Value Name or with its numeric value, for example the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause
user-request
```

will produce the same results as the command:

```
awplus(config-radsrv-group)# attribute 49 1
```

or the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause 1
```

You can define more than one instance of an attribute name (or id) by using the **repeated** parameter. For example:

```
awplus(config-radsrv-group)# attribute repeated
Nas-filter-Rule "deny in tcp from any to 0.0.0.0/0 23”
awplus(config-radsrv-group)# attribute repeated
Nas-filter-Rule "deny in tcp from any to fe80::b1 23"
```

Examples To define the attribute name ‘Service-Type’ with Administrative User (6) to the RADIUS User Group ‘Admin’, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# attribute Service-Type 6
```

To delete the attribute ‘Service-Type’ from the RADIUS User Group ‘Admin’, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# no attribute Service-Type
```

To define multiple values for attribute 'NAS-Filter-Rule', use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group dynamicAcl
awplus(config-radsrv-group)# attribute repeated
NAS-Filter-Rule "deny in tcp from any to 0.0.0.0/0 23"
awplus(config-radsrv-group)# attribute repeated
NAS-Filter-Rule "deny in tcp from any to fe80::b1 23"
```

To delete a specific value from the attribute 'NAS-Filter-Rule', use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group dynamicAcl
awplus(config-radsrv-group)# no attribute NAS-Filter-Rule "deny
in tcp from any to 0.0.0.0/0 23"
```

Related commands

egress-vlan-id

egress-vlan-name

help radius-attribute

Command changes Version 5.5.0-1.1: **repeated** parameter added

authentication

Overview Use this command to enable the specified authentication methods on the local RADIUS server.

Use the **no** variant of this command to disable specified authentication methods on the local RADIUS server.

Syntax

```
authentication {mac|eapmd5|eaptls|peap}
no authentication {mac|eapmd5|eaptls|peap}
```

Parameter	Description
mac	Enable MAC authentication method.
eapmd5	Enable EAP-MD5 authentication method.
eaptls	Enable EAP-TLS authentication method.
peap	Enable EAP-PEAP authentication method.

Default All authentication methods are enabled by default.

Mode RADIUS Server Configuration

Examples The following commands enable EAP-MD5 authentication methods on the local RADIUS server.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# authentication eapmd5
```

The following commands disable EAP-MD5 authentication methods on Local RADIUS server.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no authentication eapmd5
```

Related commands server enable

show radius local-server statistics

client (radsecproxy-srv)

Overview Use this command to add a RadSec client (for example, a NAS device) to the RadSecProxy local-server application. The application will accept RADIUS requests from all configured clients.

Use the **no** variant of this command to delete a previously-configured client from the RadSecProxy local-server application.

Syntax

```
client {<hostname>|<ip-addr>} [name-check {on|off}]
no client {<hostname>|<ip-addr>}
```

Parameter	Description	
<hostname>	Hostname of client.	
<ip-addr>	Specify the client IPv4 address, in dotted decimal notation (A.B.C.D).	
name-check	Specify whether or not to enforce certificate name checking for this client. If the parameter is not specified then the global behavior, which defaults to **on**, is used.	
	on	Enable name checking for this client.
	off	Disable name checking for this client.

Mode RadSecProxy Local Server Configuration

Usage notes The client may be specified by its domain name or by its IPv4 address. If a domain name is used, it must be resolvable using a configured DNS name server.

Each client may be configured to use certificate name-checking; if not specified, the global behavior defined by **client name-check** or **no client name-check** will be used. If name checking is enabled, the Common Name portion of the subject field of the client's X.509 certificate must match the domain name or IP address specified in this command.

NOTE: *If mutual authentication is disabled then this parameter has no effect, see the client mutual-authentication command.*

Example To add a client called 'mynas.local' with certificate name checking **off**, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)# client mynas.local name-check
off
```

Related commands

client mutual-authentication

client name-check

client trustpoint

radius-secure-proxy local-server

client mutual-authentication

Overview This command enables or disables mutual certificate authentication for all RadSecProxy clients. When enabled, the RadSecProxy local-server application will request and validate an X.509 certificate from the client when establishing a connection.

The **no** variant of this command disables mutual certificate validation. The local-server application will still transmit the local server certificate to the client, but will not expect or validate a certificate from the client.

Syntax

```
client mutual-authentication
no client mutual-authentication
```

Default Mutual authentication is enabled by default.

Mode RadSecProxy Local Server Configuration

Example Disable mutual certificate validation with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)# no client
mutual-authentication
```

Related commands

client (radsecproxy-srv)

client name-check

radius-secure-proxy local-server

Command changes Version 5.4.6-2.1: command added

client name-check

Overview This command sets the global behavior for certificate name-checking for the RadSecProxy localserver application to **on**. This behavior will be used for all clients associated with the application that do not specify a behavior on a per-client basis. If name-checking is enabled, the Common Name portion of the subject field of the client's X.509 certificate must match the domain name or IP address specified in the **client (radsecproxy-aaa)** command.

Use the **no** variant of this command to set the global behavior for certificate name checking to **off**

Syntax

```
client name-check
no client name-check
```

Default Certificate name checking is on by default.

Mode RadSecProxy Local Server Configuration

Example Disable certificate name checking globally with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)# no client name-check
```

Related commands

client (radsecproxy-srv)

client trustpoint

radius-secure-proxy local-server

client trustpoint

Overview This command adds one or more trustpoints to be used with the RadSecProxy local-server application. Multiple trustpoints may be specified, or the command may be executed more than once, to add multiple trustpoints to the application.

The **no** version of this command removes one or more trustpoints from the list of trustpoints associated with the application.

Syntax

```
client trustpoint [<trustpoint-list>]
no client trustpoint [<trustpoint-list>]
```

Parameter	Description
<trustpoint-list>	Specify one or more trustpoints to be added or deleted.

Mode RadSecProxy Local Server Configuration

Usage notes The device certificate associated with the first trustpoint added to the application will be transmitted to remote servers. The certificate received from the remote server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

If you enter **client trustpoint** without specifying a trustpoint, the trustpoint list will be unchanged.

If you enter **no client trustpoint** without specifying a trustpoint, all trustpoints will be disassociated from the application.

Example You can add multiple trustpoints to the RadSecProxy local-server by executing the command multiple times:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)# client trustpoint example_1
awplus(config-radsecproxy-srv)# client trustpoint example_2
```

Alternatively, add multiple trustpoints with a single command:

```
awplus(config-radsecproxy-srv)# client trustpoint example_3
example_4
```

Disassociate all trustpoints from the RadSecProxy local-server application using the command:

```
awplus(config-radsecproxy-srv)# no client trustpoint
```

Related commands

client (radsecproxy-srv)

client name-check

radius-secure-proxy local-server

clear radius local-server statistics

Overview Use this command to clear the statistics stored on the device for the local RADIUS server.

Use this command without any parameters to clear all types of local RADIUS server statistics.

Syntax

```
clear radius local-server statistics [nas|server|user]
```

Parameter	Description
`nas`	Clear the NAS (Network Access Server) statistics on the device. For example, clearing statistics stored for NAS server invalid passwords.
`server`	Clear the Local RADIUS Server statistics on the device. For example, clearing Local RADIUS Servers statistics for all failed login attempts.
`user`	Clear the Local RADIUS Server user statistics. For example, clearing statistics stored for the number of successful user logins.

Mode Privileged Exec

Usage Refer to the sample output for the show radius local-server statistics for further information about the type of statistics each parameter option for this command clears. Both the **nas** and **server** parameters clear unknown username and invalid passwords statistics, while the `user` parameter clears the number of successful and failed logins for each local RADIUS server user.

Examples To clear the NAS (Network Access Server) statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics nas
```

To clear the local RADIUS server statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics server
```

To clear the local RADIUS server user statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics user
```

Related commands show radius local-server statistics

copy fdb-radius-users (to file)

Overview Use this command to create a set of local RADIUS server users from MAC addresses in the local FDB. A local RADIUS server user created using this command can be used for MAC authentication.

Syntax

```
copy fdb-radius-users
{local-radius-user-db|nvs|flash|usb|debug|tftp|scp|
fserver|<url>} [interface <port>] [vlan <vid>] [group <name>]
[export-vlan [<radius-group-name>]]
```

Parameter	Description
`local-radius-user-db`	Copy the local RADIUS server users created to the local RADIUS server.
`nvs`	Copy the local RADIUS server users created to NVS memory.
`flash`	Copy the local RADIUS server users created to Flash memory.
`usb`	Copy the local RADIUS server users created to USB storage device.
`debug`	Copy the local RADIUS server users created to debug.
`tftp`	Copy the local RADIUS server users created to the TFTP destination.
`scp`	Copy the local RADIUS server users created to the SCP destination.
`fserver`	Copy the local RADIUS server users created to the remote file server.
`<url>`	Copy the local RADIUS server users created to the specified URL.
`interface <port>`	Copy only MAC addresses learned on a specified device port. Wildcards may be used when specifying an interface name.
`vlan <vid>`	Copy only MAC addresses learned on a specified VLAN.
`group <name>`	Assign a group name to the local RADIUS server users created.
`export-vlan`	Export VLAN ID assigned to exported FDB entry.
`<radius-group-name>`	Prefix for Radius group name storing VLAN ID

Mode Privileged Exec

Usage notes The local RADIUS server users created are written to a specified destination file in local RADIUS user CSV (Comma Separated Values) format. The local RADIUS server users can then be imported to a local RADIUS server using the copy local-radius-user-db (from file) command.

The name and password of the local RADIUS server users created use a MAC address, which can be used for MAC authentication.

This command does not copy a MAC address learned by the CPU or the management port.

This command can filter FDB entries by the interface name and the VLAN ID. When the interface name and the VLAN ID are specified, this command generates local RADIUS server users from only the MAC address learned on the specified interface and on the specified VLAN.

Examples To register the local RADIUS server users from the local FDB directly to the local RADIUS server, use the command:

```
awplus# copy fdb-radius-users local-radius-user-db
```

To register the local RADIUS server users from the interface port1.0.1 to the local RADIUS server, use the command:

```
awplus# copy fdb-radius-users local-radius-user-db interface
port1.0.1
```

To copy output generated as local RADIUS server user data from MAC addresses learned on vlan10 on interface port1.0.1 to the file radius-user.csv, use the command:

```
awplus# copy fdb-radius-users radius-user.csv interface
port1.0.1 vlan10
```

To copy output generated as local RADIUS server user data from MAC addresses learned on vlan10 on interface port1.0.1 to a file on the remote file server, use the command:

```
awplus# copy fdb-radius-users fserver interface port1.0.1
vlan10
```

Related commands copy local-radius-user-db (to file)

copy local-radius-user-db (from file)

copy local-radius-user-db (from file)

Overview Use this command to copy the Local RADIUS server user data from a file. The file, including the RADIUS user data in the file, must be in the CSV (Comma Separated Values) format.

You can select **add** or **replace** as the copy method. The **add** parameter option copies the contents of specified file to the local RADIUS server user database. If the same user exists then the old user is removed before adding a new user. The **replace** parameter option deletes all contents of the local RADIUS server user database before copying the contents of specified file.

Syntax

```
copy <source-url> local-radius-user-db [add|replace]
```

Parameter	Description
<source-url>	URL of the source file.
`add`	Add file contents to local RADIUS server user database.
`replace`	Replace current local RADIUS server user database with file contents.

Default When no copy method is specified with this command the **replace** option is applied.

Mode Privileged Exec

Examples To replace the current local RADIUS server user data to the contents of http://datahost/ user.csv, use the following command:

```
awplus# copy http://datahost/user.csv local-radius-user-db
```

To add the contents of http://datahost/user.csv to the current local RADIUS server user database, use the following command:

```
awplus# copy http://datahost/user.csv local-radius-user-db add
```

Related commands copy fdb-radius-users (to file)

copy local-radius-user-db (to file)

copy local-radius-user-db (to file)

Overview Use this command to copy the local RADIUS server user data to a file. The output file produced is CSV (Comma Separated Values) format.

Syntax

```
copy local-radius-user-db
{nvs|flash|usb|tftp|scp|<destination-url>}
```

Parameter	Description
`nvs`	Copy to NVS memory.
`flash`	Copy to Flash memory.
`usb`	Copy to USB storage device.
`tftp`	Copy to TFTP destination.
`scp`	Copy to SCP destination.
<destination-url>	URL of the Destination file.

Mode Privileged Exec

Example Copy the current local RADIUS server user data to http://datahost/user.csv.

```
awplus# copy local-radius-user-db http://datahost/user.csv
```

Related commands

copy fdb-radius-users (to file)

copy local-radius-user-db (from file)

crypto pki enroll local (deleted)

Overview This command is no longer available. Please use the following command instead:

```
crypto pki enroll <trustpoint>
```

Note that "local" is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

crypto pki enroll local local-radius-all-users (deleted)

Overview This command is no longer available. Please use the following command instead:

```
crypto pki enroll <trustpoint> local-radius-all-users
```

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

crypto pki enroll local user (deleted)

Overview This command is no longer available. Please use the following command instead:

```
crypto pki enroll <trustpoint> user <username>
```

Note that "local" is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

crypto pki export local pem (deleted)

Overview This command is no longer available. Please use the crypto pki export pem command instead:

```
crypto pki export <trustpoint> pem [terminal|<url>]
```

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

crypto pki export local pkcs12 (deleted)

Overview This command is no longer available. Please use the crypto pki export pkcs12 command instead:

```
crypto pki export <trustpoint> pkcs12 {ca|server|<username>}
<url>
```

Note that "local" is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

crypto pki trustpoint local (deleted)

Overview This command is no longer available. Please use the following command instead:

```
crypto pki trustpoint <trustpoint>
```

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

debug crypto pki (deleted)

Overview This command is no longer available.

domain-style

Overview Use this command to enable a specified domain style on the local RADIUS server. The local RADIUS server decodes the domain portion of a username login string when this command is enabled.

Use the **no** variant of this command to disable the specified domain style on the local RADIUS server.

Syntax

```
domain-style {suffix-atsign|ntdomain}
no domain-style {suffix-atsign|ntdomain}
```

Parameter	Description
`suffix-atsign`	Enable at sign "@" delimited suffix style, i.e. "user@domain".
`ntdomain`	Enable NT domain style, i.e. "domain\user".

Default This feature is disabled by default.

Mode RADIUS Server Configuration

Usage notes When both domain styles are enabled, the first domain style configured has the highest priority. A username login string is matched against the first domain style enabled. Then, if the username login string is not decoded, it is matched against the second domain style enabled.

Examples To enable NT domain style on the local RADIUS server, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# domain-style ntdomain
```

To disable NT domain style on the local RADIUS server, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no domain-style ntdomain
```

Related commands server enable

egress-vlan-id

Overview Use this command to configure the standard RADIUS attribute "Egress-VLANID (56)" for the local RADIUS Server user group.

Use the **no** variant of this command to remove the Egress-VLANID attribute from the local RADIUS server user group.

Syntax

```
egress-vlan-id <vid> [tagged|untagged]
no egress-vlan-id
```

Parameter	Description
`<vid>`	The VLAN identifier to be used for the Egress VLANID attribute, in the range 1 to 4094.
`tagged`	Set frames on the VLAN as tagged. This sets the tag indication field to indicate that all frames on this VLAN are tagged.
`untagged`	Set all frames on the VLAN as untagged. This sets the tag indication field to indicate that all frames on this VLAN are untagged.

Default By default, no Egress-VLANID attributes are configured.

Mode RADIUS Server Group Configuration

Usage When a Voice VLAN is configured for dynamic VLAN allocation (switchport voice vlan command), the RADIUS server must be configured to send the VLAN information when an IP phone is successfully authenticated. Use either the egress-vlan-id command or the egress-vlan-name command, and specify the **tagged** parameter.

Examples To set the "Egress-VLANID" attribute for the *NormalUsers* local RADIUS server user group to VLAN identifier 200, with tagged frames, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# egress-vlan-id 200 tagged
```

To remove the "Egress-VLANID" attribute for the *NormalUsers* local RADIUS server user group, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no egress-vlan-id
```

Related commands

attribute

egress-vlan-name

switchport voice vlan

egress-vlan-name

Overview Use this command to configure the standard RADIUS attribute "Egress-VLAN-Name (58)" for the local RADIUS server user group.

Use the **no** variant of this command to remove the Egress-VLAN-Name attribute from the local RADIUS server user group.

Syntax

```
egress-vlan-name <vlan-name> [tagged|untagged]
no egress-vlan-name
```

Parameter	Description
<vlan-name>	The VLAN name to be configured as the Egress-VLAN-Name attribute.
`tagged`	Set frames on the VLAN as tagged. This sets the tag indication field to indicate that all frames on this VLAN are tagged.
`untagged`	Set all frames on the VLAN as untagged. This sets the tag indication field to indicate that all frames on this VLAN are untagged.

Default By default, no Egress-VLAN-Name attributes are configured.

Mode RADIUS Server Group Configuration

Usage When a Voice VLAN is configured for dynamic VLAN allocation (switchport voice vlan command), the RADIUS server must be configured to send the VLAN information when an IP phone is successfully authenticated. Use either the egress-vlan-id command or the egress-vlan-name command, and specify the **tagged** parameter.

Examples To configure the "Egress-VLAN-Name" attribute for the RADIUS server user group *NormalUsers* with the VLAN name *vlan2* and all frames on this VLAN tagged, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# egress-vlan-name vlan2 tagged
```

To delete the "Egress-VLAN-Name" attribute for the *NormalUsers* group, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no egress-vlan-name
```

Related commands

attribute

egress-vlan-id

switchport voice vlan

group

Overview Use this command to create a local RADIUS server user group, and enter local RADIUS Server User Group Configuration mode.

Use the **no** variant of this command to delete the local RADIUS server user group.

Syntax

```
group <user-group-name>
no group <user-group-name>
```

Parameter	Description
<user-group-name>	User group name string.

Mode RADIUS Server Configuration

Examples The following command creates the user group NormalUsers.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
```

The following command deletes user group NormalUsers.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no group NormalUsers
```

Related commands

user (RADIUS server)

show radius local-server user

vlan (RADIUS server)

nas

Overview This command adds a client device (the Network Access Server or the NAS) to the list of devices that are able to send authentication requests to the local RADIUS server. The NAS is identified by its IP address and a shared secret (also referred to as a shared key) must be defined that the NAS will use to establish its identity.

Use the **no** variant of this command to remove a NAS client from the list of devices that are allowed to send authentication requests to the local RADIUS server.

Syntax

```
nas <ip-address> key <nas-keystring>
no nas <ip-address>
```

Parameter	Description
<ip-address>	RADIUS NAS IP address.
<nas-keystring>	NAS shared keystring.

Mode RADIUS Server Configuration

Examples The following commands add the NAS with an IP address of `192.168.1.2` to the list of clients that may send authentication requests to the local RADIUS server. Note the shared key that this NAS will use to establish its identify is `NAS_PASSWORD`.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# nas 192.168.1.2 key NAS_PASSWORD
```

The following commands remove the NAS with an IP address of `192.168.1.2` from the list of clients that are allowed to send authentication requests to the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no nas 192.168.1.2
```

Related commands show radius local-server nas

help radius-attribute

Overview Use this command to display a list of standard and vendor specific valid RADIUS attributes that are supported by the local RADIUS server.

Syntax

```
help radius-attribute [<attribute-name>|<attribute-ID>]
```

Parameter	Description
<attribute-name>	List the details and predefined values for the named attribute.
<attribute-ID>	List the details and predefined values for the given attribute ID.

Mode Privileged Exec

Usage notes When used without a parameter, this command lists all of the available RADIUS attributes.

When used with an attribute name or ID, this command displays the attribute name, value type, and any predefined values.

Example To list all available RADIUS attributes, use the following command:

```
awplus# help radius-attribute
```

```
awplus#help radius-attribute
Standard Attributes:
  1      User-Name
  2      User-Password
  3      CHAP-Password
  4      NAS-IP-Address
  5      NAS-Port
  6      Service-Type
...
```

To display the details for the RADIUS attribute Frag-Status, use the following command:

```
awplus# help radius-attribute frag-status
```

```
awplus#help radius-attribute frag-status
Frag-Status : integer (Integer number)

Pre-defined values :
    Fragmentation-Supported (1)
    More-Data-Pending (2)
    More-Data-Request (3)
    Reserved (0)
```

Related commands attribute

Command changes Version 5.4.8-0.2: command added

Version 5.4.9-0.1: added to x530 Series products

radius-secure-proxy local-server

Overview Use this command to enter the RadSecProxy local-server application configuration mode. This application allows remote RadSec clients to communicate with the local RADIUS server process via a secure (TLS) proxy.

Syntax

```
radius-secure-proxy local-server
```

Mode Global Configuration Mode

Example To change mode from User Exec mode to the RadSecProxy local-server configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)#
```

Related commands

client (radsecproxy-srv)

client name-check

client trustpoint

radius-server local

Overview Use this command to navigate to the Local RADIUS server configuration mode `(config-radsrv)` from the Global Configuration mode `(config)`.

Syntax

```
radius-server local
```

Mode Global Configuration

Example Local RADIUS Server commands are available from `config-radsrv` configuration mode. To change mode from User Exec mode to the Local RADIUS Server mode (config- radsrv), use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)#
```

Output

```
awplus(config)#radius-server local
Creating Local CA repository.....OK
Enrolling Local System to local trustpoint..OK
awplus(config-radsrv)#
```

Related commands

server enable

show radius local-server group

show radius local-server nas

show radius local-server statistics

show radius local-server user

server auth-port

Overview Use this command to change the UDP port number for local RADIUS server authentication.

Use the **no** variant of this command to reset the RADIUS server authentication port back to the default.

Syntax

```
server auth-port <1-65535>
no server auth-port
```

Parameter	Description
<1-65535>	UDP port number.

Default The default local RADIUS server UDP authentication port number is 1812.

Mode RADIUS Server Configuration

Examples The following commands set the RADIUS server authentication port to 10000.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# server auth-port 10000
```

The following commands reset the RADIUS server authentication port back to the default UDP port of 1812.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no server auth-port
```

Related commands server enable

show radius local-server statistics

server enable

Overview This command enables the local RADIUS server. The local RADIUS server feature is started immediately when this command is issued.

The **no** variant of this command disables local RADIUS server. When this command is issued, the local RADIUS server stops operating.

Syntax

```
server enable
no server enable
```

Default The local RADIUS server is disabled by default and must be enabled for use with this command.

Mode RADIUS Server Configuration

Examples To enable the local RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# server enable
```

To disable the local RADIUS server, use the command:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no server enable
```

Related commands server auth-port

show radius local-server statistics

show radius local-server group

Overview Use this command to display information about the local RADIUS server user group.

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

Syntax

```
show radius local-server group [<user-group-name>]
```

Parameter	Description
<user-group-name>	User group name string.

Mode User Exec and Privileged Exec

Example The following command displays Local RADIUS server user group information.

```
awplus# show radius local-server group
```

Output

Table 1: Example output from the **show radius local-server group** command

```
Group-Name          Vlan
-------------------------------------------------------------
NetworkOperators    ManagementNet
NormalUsers         CommonNet
```

Table 2: Parameters in the output of the **show radius local-server group** command

Parameter	Description
Group-Name	Group name.
Vlan	VLAN name assigned to the group.

Related commands group

show radius local-server nas

Overview Use this command to display information about NAS (Network Access Servers) registered to the local RADIUS server.

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

Syntax

```
show radius local-server nas [<ip-address>]
```

Parameter	Description
<ip-address>	Specify NAS IP address for show output.

Mode User Exec and Privileged Exec

Example The following command displays NAS information.

```
awplus# show radius local-server nas
```

Output

Table 3: Example output from the **show radius local-server nas** command

```
NAS-Address      Shared-Key
-----------------------------------------------------
127.0.0.1       awplus-local-radius-server
```

Table 4: Parameters in the output of the **show radius local-server nas** command

Parameter	Description
NAS-Address	IP address of NAS.
Shared-Key	Shared key used for RADIUS connection.

Related commands nas

show radius local-server statistics

Overview Use this command to display statistics about the local RADIUS server.

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

Syntax

```
show radius local-server statistics
```

Mode User Exec and Privileged Exec

Usage notes Both unknown usernames and invalid passwords will display as failed logins in the show output.

Example The following command displays Local RADIUS server statistics.

```
awplus# show radius local-server statistics
```

Output

Table 5: Example output from the **show radius local-server statistics** command

```
Server status       : Run (administrative status is enable)
Enabled methods     : MAC EAP-MD5 EAP-TLS EAP-PEAP
Available methods   : MAC EAP-MD5 EAP-TLS EAP-PEAP
EAP trustpoints     : local

Successes              :1              Unknown NAS             :0
Failed Logins          :0              Invalid packet from NAS :0
Internal Error         :0              Unknown Error           :0

NAS : 127.0.0.1
Successes              :0              Shared key mismatch     :0
Failed Logins          :0              Unknown RADIUS message  :0
Unknown EAP message    :0              Unknown EAP auth type   :0
Corrupted packet       :0

NAS : 192.168.1.61
Successes              :0              Shared key mismatch     :0
Failed Logins          :0              Unknown RADIUS message  :0
Unknown EAP message    :0              Unknown EAP auth type   :0
Corrupted packet :0

Username  Successes  Failures
Tom               1         0
admin             0         0
```

Related commands

clear radius local-server statistics

radius-server local

server enable

server auth-port

show radius local-server user

Overview Use this command to display information about the local RADIUS server user.

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

Syntax

```
show radius local-server user [<user-name>]
show radius local-server user [<user-name>] format csv
show radius local-server user [<user-name>] detail
```

Parameter	Description
`<user-name>`	RADIUS user name. If no user name is specified, information for all users is displayed.
`format csv`	Format output as CSV. This parameter is only available in Privileged Exec mode.
`detail`	Display detailed information about the user.

Mode User Exec and Privileged Exec

Examples The following command displays Local RADIUS server user information for user Tom.

```
awplus# show radius local-server user Tom
```

Table 6: Example output from the **show radius local-server user** command

```
User-Name            Group               Vlan
-------------------------------------------------------------
Tom                  NetworkOperators    ManagementNet
```

The following command displays all Local RADIUS server information for all users.

```
awplus# show radius local-server user
```

The following command displays Local RADIUS server user information for Tom in CSV format (only available in Privileged Exec mode).

```
awplus# show radius local-server user Tom format csv
```

Table 7: Example output from the **show radius local-server user Tom format csv** command

```
true,"NetworkOperators","Tom","abcd",0,2099/01/01,1,"","","Managem
entNet"false,3600,false,0,"",false,"",false,false,"","","",false,f
alse,false,,false,0,0,"",true
```

The following command displays detailed Local RADIUS server user information for all users.

```
awplus# show radius local-server user detail
```

Table 8: Example output from the **show radius local-server user detail** command

```
awplus# show radius local-server user detail
Total users: 1
Maximum users allowed by license: 3
----------------------------------------------------------------
    Username  : Tom
      Group   : NetworkOperators
      Vlan    : VlanName
```

Table 9: Parameters in the output from the **show radius local-server user** command

Parameter	Description
User-Name	User name.
Group	Group name assigned to the user.
Vlan	VLAN name assigned to the user.

Related commands

group

user (RADIUS server)

Command changes

Version 5.4.9-0.1: **detail** parameter added

user (RADIUS server)

Overview Use this command to register a user to the local RADIUS server.

Use the **no** variant of this command to delete a user from the local RADIUS server.

Syntax

```
user <radius-user-name> [encrypted] password <user-password>
[group <user-group>]
```

```
no user <radius-user-name>
```

Parameter	Description
<radius-user-name>	RADIUS user name. This can also be a MAC address in the IEEE standard format of `HH-HH-HH-HH-HH-HH` if you are configuring MAC authentication to use local RADIUS server.
`encrypted`	Specifies that the password is being entered in its encrypted form, so that it is not further encrypted. When creating a new user, enter the password in plaintext, and do not use the **encrypted** parameter. Use the **encrypted** parameter only when referring to a user that has previously been created. For instance, when adding an existing user from another RADIUS server, use the **encrypted** parameter, and enter the encrypted version of the password that appears in the output of **show** commands for the user.
<user-password>	User password. This can also be a MAC address in the IEEE standard format of `HH-HH-HH-HH-HH-HH` if you are configuring MAC authentication to use local RADIUS server.
`group`	Specify the group for the user.
<user-group>	User group name.

Mode RADIUS Server Configuration

Usage notes RADIUS user names cannot contain question mark (`?`), space ( ), or quote (“ “) characters. RADIUS user names containing the below characters cannot use certificate authentication:

```
/ \ '$ &()*;< > '|
```

Certificates cannot be created and exported for RADIUS user names that contain the above characters. We advise you to avoid using these characters in RADIUS user names if you need to use certificate authentication, because you will not be able to create and export certificates.

You also can use the IEEE standard format hexadecimal notation (`HH-HH-HH-HH-HH-HH`) to specify a supplicant MAC address to configure the user name and user password parameters to use local RADIUS server for MAC Authentication. See the AAA and Port_Authentication Feature Overview and Configuration_Guide for a sample MAC configuration. See also the command **user**

00-db-59-ab-70-37 password 00-db-59-ab-70-37 as shown in the command examples.

Examples

The following commands add user "Tom" to the local RADIUS server and sets his password to "QwerSD".

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user Tom password QwerSD
```

The following commands add user "Tom" to the local RADIUS server user group "NormalUsers" and sets his password "QwerSD".

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user Tom password QwerSD group
NormalUsers
```

The following commands remove user "Tom" from the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no user Tom
```

The following commands add the supplicant MAC address 00-d0-59-ab-70-37 to the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user 00-db-59-ab-70-37 password
00-db-59-ab-70-37
```

The following commands remove the supplicant MAC address 00-d0-59-ab-70-37 from the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no user 00-db-59-ab-70-37
```

Related commands

group

show radius local-server user

vlan (RADIUS server)

Overview Use this command to set the VLAN ID or name for the local RADIUS server user group. The VLAN information is used for authentication with the dynamic VLAN feature.

Use the **no** variant of this command to clear the VLAN ID or VLAN name for the local RADIUS server user group.

Syntax

```
vlan {<vid>|<vlan-name>}
no vlan
```

Parameter	Description
<vid>	VLAN ID.
<vlan-name>	VLAN name.

Default VLAN information is not set by default.

Mode RADIUS Server Group Configuration

Examples The following commands set VLAN ID 200 to the group named *NormalUsers*:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# vlan 200
```

The following commands remove VLAN ID 200 from the group named *NormalUsers*:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no vlan
```

Related commands

group

show radius local-server user

48 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 2407
- "crypto key zeroize" on page 2408
- "crypto pki authenticate" on page 2409
- "crypto pki enroll" on page 2410
- "crypto pki enroll user" on page 2411
- "crypto pki export pem" on page 2413
- "crypto pki export pkcs12" on page 2414
- "crypto pki import pem" on page 2416
- "crypto pki import pkcs12" on page 2418
- "crypto pki trustpoint" on page 2419
- "crypto secure-mode" on page 2420
- "crypto secure-mode delete hostkey" on page 2421
- "crypto verify" on page 2422
- "enrollment (ca-trustpoint)" on page 2424
- "fingerprint (ca-trustpoint)" on page 2425
- "no crypto pki certificate" on page 2427
- "rsakeypair (ca-trustpoint)" on page 2428
- "show crypto key mypubkey rsa" on page 2429
- "show crypto pki certificates" on page 2430

- "show crypto pki enrollment user" on page 2432
- "show crypto pki trustpoint" on page 2433
- "show secure-mode" on page 2434
- "subject-name (ca-trustpoint)" on page 2435

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>] [<1024-4096>]
```

Parameter	Description
<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.
<1024-4096>	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 4096 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 2048, use the commands:

```
awplus> enable
awplus# crypto key generate rsa label example-server-key 2048
```

Related commands

crypto key zeroize

rsakeypair (ca-trustpoint)

show crypto key mypubkey rsa

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 When the system is in secure mode, this command will securely delete the file (the file's sectors in NVS will be overwritten with random data three times before deletion). When the device is not in secure mode, 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

crypto secure-mode

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 tobe 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

crypto secure-mode

Overview Use this command to put the device into Secure Mode. When in Secure Mode, the following are disabled:

- Telnet
- SSHv1
- SNMPv1/v2
- All privilege levels except 1 and 15
- Algorithms that are not supported under FIPS, including MD5, RSA-1 and DSA
- The ability to store passwords in cleartext and to specify an **enable** password.

In Secure Mode, the web server on the device (used by the Device GUI) only accepts AES128-SHA ciphers.

Note: Stacking is not supported in Secure Mode.

Use the **no** variant of this command to leave Secure Mode. You should delete all sensitive information first; see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
crypto secure-mode
no crypto secure-mode
```

Default By default, the device is not in Secure Mode.

Mode Global Configuration

Example For step-by-step instructions about how to enter and leave Secure Mode, see “How to Enable Secure Mode” in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Related commands

boot system

crypto key zeroize

crypto pki trustpoint

crypto verify

show secure-mode

Command changes

Version 5.4.6-1.1: command added to x930 Series

Version 5.4.8-1.2: command added to x220, XS900MX, x550 Series

Version 5.4.8-2.1: command added to SBx908 GEN2, x950 Series

crypto secure-mode delete hostkey

Overview Use this command to delete the encryption key used for securing configuration secrets in secure mode. Note that doing this will make these secrets impossible to decrypt, potentially impacting the device configuration.

Syntax
```
crypto secure-mode delete hostkey
```

Default Not set.

Mode Privileged Exec

Example To delete the encrypted key, use the command:

```
awplus# crypto secure-mode delete hostkey
```

Related commands
radius-server host

radius-server key

ntp authentication-key

crypto secure-mode

Command changes Version 5.4.9-2.1: command added

crypto verify

Overview Use this command to compare the SHA256 checksum of the release file or bootloader with the correct checksum for the file. This ensures that the release file or bootloader has not been corrupted or interfered with during download.

Use the **no** variant of this command to remove a verified filename/hash combination from the running configuration.

Syntax

```
crypto verify <filename> <hash-value>
crypto verify signed <filename> <hash-value>
crypto verify bootrom <hash-value>
no crypto verify <filename>
```

Parameter	Description
<filename>	The AlliedWare Plus release file that you want to verify
<hash-value>	The known correct checksum of the file. The correct checksum is listed in the release sha256sum file, which is available from the Allied Telesis Download Center.
signed	The hash used is from a <release>.sig file and calculated as a keyed HMAC-SHA. Only use this parameter in accordance with the Allied Telesis FIPS Security Policy.
bootrom	This tells the device that the signature provided is for the bootrom. It stores that hash permanently, preventing boot if the bootloader is modified.

Default No default

Mode Global Configuration

Usage notes If the verification fails, the following error message will be generated:

```
% Verification Failed
```

If the verification fails, please delete the release file and contact Allied Telesis support.

All models of a particular series run the same release file and therefore have the same checksum. For example, all x930 Series switches have the same checksum.

Once the device has successfully verified the release file, it adds the **crypto verify** command to the running configuration.

If the device is in secure mode, it will verify the release file every time it boots up. To do this, it runs the **crypto verify** command while booting. Therefore, you need to copy the **crypto verify** command to the startup configuration, by using the command **copy running-config startup-config**. If the **crypto verify** command is not in the startup configuration, the device will report a verification error at bootup.

If there is a verification error at bootup, the device produces an error message and finishes booting up. If this happens, run the **crypto verify** command after bootup finishes, to verify the running release file. If verification of the running release file fails, delete the release file and contact Allied Telesis support.

Caution:

When using signature verification, if:

- the release verified is the boot release
- and the device is running in secure mode
- and signed verification succeeds

then the signed hash is also stored into the device and enforced on all subsequent boots.

This means that if you change the software version, the switch will not boot up. You can only change the software version if you reset the switch to the factory defaults **before** changing the software version, by using the command erase factory-default.

Example To verify the release file for 5.4.8-1.2 on an x930 Series switch, use the commands:

```
awplus# configure terminal
awplus(config)# crypto verify x930-5.4.8-1.2.rel
50fae963b460ba02eb0bd609289c0491de404ba5b0d7e5fa79e64f56082ecf
ee
```

Related commands crypto secure-mode

show secure-mode

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 48-1: 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 48-2: 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 48-3: 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 48-4: 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 secure-mode

Overview Use this command to see whether secure mode is enabled or not. Secure mode disables a number of insecure features, such as Telnet.

Syntax

```
show secure-mode
```

Mode User Exec/Privileged Exec

Example To see if secure mode is enabled, use the command:

```
awplus# show secure-mode
```

Output Figure 48-5: Example output from **show secure-mode**

```
awplus#show secure-mode
Secure mode is enabled
```

Related commands crypto secure-mode

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

49 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.

TACACS+ is not available in Secure Mode (see the crypto secure-mode command).

Command List

- "aaa authorization commands" on page 2438
- "aaa authorization config-commands" on page 2440
- "authorization commands" on page 2441
- "ip tacacs source-interface" on page 2443
- "show tacacs+" on page 2444
- "tacacs-server host" on page 2446
- "tacacs-server key" on page 2448
- "tacacs-server timeout" on page 2449

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 49-1: 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+

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+

50 DHCP Snooping Commands

Introduction

Overview

This chapter gives detailed information about the commands used to configure DHCP snooping. For detailed descriptions of related ACL commands, see IPv4 Hardware Access Control List (ACL) Commands. For more information about DHCP snooping, see the DHCP Snooping Feature Overview and Configuration Guide.

DHCP snooping can operate on static link aggregators (e.g. sa2) and dynamic link aggregators (e.g. po2), as well as on switch ports (e.g. port1.0.2).

Command List

- "arp security" on page 2452
- "arp security drop link-local-arps" on page 2453
- "arp security violation" on page 2454
- "clear arp security statistics" on page 2456
- "clear ip dhcp snooping binding" on page 2457
- "clear ip dhcp snooping statistics" on page 2458
- "debug arp security" on page 2459
- "debug ip dhcp snooping" on page 2460
- "ip dhcp snooping" on page 2461
- "ip dhcp snooping agent-option" on page 2463
- "ip dhcp snooping agent-option allow-untrusted" on page 2464
- "ip dhcp snooping agent-option circuit-id vlantriplet" on page 2465
- "ip dhcp snooping agent-option remote-id" on page 2466
- "ip dhcp snooping binding" on page 2467
- "ip dhcp snooping database" on page 2468
- "ip dhcp snooping delete-by-client" on page 2469
- "ip dhcp snooping delete-by-linkdown" on page 2470

- "ip dhcp snooping max-bindings" on page 2471
- "ip dhcp snooping subscriber-id" on page 2472
- "ip dhcp snooping trust" on page 2473
- "ip dhcp snooping verify mac-address" on page 2474
- "ip dhcp snooping violation" on page 2475
- "ip source binding" on page 2476
- "service dhcp-snooping" on page 2478
- "show arp security" on page 2480
- "show arp security interface" on page 2481
- "show arp security statistics" on page 2483
- "show debugging arp security" on page 2485
- "show debugging ip dhcp snooping" on page 2486
- "show ip dhcp snooping" on page 2487
- "show ip dhcp snooping acl" on page 2488
- "show ip dhcp snooping agent-option" on page 2491
- "show ip dhcp snooping binding" on page 2493
- "show ip dhcp snooping interface" on page 2495
- "show ip dhcp snooping statistics" on page 2497
- "show ip source binding" on page 2500

arp security

Overview Use this command to enable ARP security on untrusted ports in the VLANs, so that the switch only responds to/forwards ARP packets if they have recognized IP and MAC source addresses.

Use the **no** variant of this command to disable ARP security on the VLANs.

Syntax

```
arp security
no arp security
```

Default Disabled

Mode Interface Configuration (VLANs)

Usage Enable ARP security to provide protection against ARP spoofing. DHCP snooping must also be enabled on the switch (service dhcp-snooping command), and on the VLANs (ip dhcp snooping command).

Example To enable ARP security on VLANs 2 to 4, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# arp security
```

Related commands

arp security violation

show arp security

show arp security interface

show arp security statistics

arp security drop link-local-arps

Overview Use this command to enable ARP security on a per-port basis. This means that IPv4 link-local ARPs will be dropped without causing an ARP security violation when received.

Use the **no** variant of this command to return to the default setting of disabled.

Syntax

```
arp security drop link-local-arps
no arp security drop link-local-arps
```

Default Disabled by default.

Mode Interface Configuration

Usage notes Hosts that implement RFC 3927 may automatically assign themselves link-local IPv4 addresses in the subnet 169.254.0.0/16, if they are configured to learn their IP addresses via DHCP but are unable to contact a DHCP server. This is common behavior for all versions of Microsoft Windows since Windows XP. In an attempt to avoid IP address collision with other devices on the local network, the host will broadcast ARP probes for its randomly selected link-local IP address.

By default, ARP security will treat these ARP probes as violations and carry out the configured violation action on the port they are received on. If the violation action is configured as link-down, this will result in the host being disconnected from the network, which will interrupt any DHCP IP address discovery that was in progress.

Use this command to configure ARP Security to drop these ARP probes, and any other ARPs that contain link-local IP addresses, without raising a violation on the affected port. The count of ARPs dropped in this manner can be seen in the output of **show arp security statistics detail**.

Example To configure ARP security to drop IPv4 link local ARPs on port1.0.1 to port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# arp security drop link-local-arps
```

Related commands

arp security

arp security violation

show arp security statistics

Command changes Version 5.4.9-1.1: command added.

arp security violation

Overview Use this command to specify an additional action to perform if an ARP security violation is detected on the ports. ARP security must also be enabled (arp security command).

Use the **no** variant of this command to remove the specified action, or all actions. Traffic violating ARP security will be dropped, but no other action will be taken.

Syntax

```
arp security violation {log|trap|link-down} ...
no arp security violation [log|trap|link-down] ...
```

Parameter	Description
`log`	Generate a log message. To display these messages, use the show log command.
`trap`	Generate an SNMP notification (trap). To send SNMP notifications, SNMP must also be configured, and DHCP snooping notifications must be enabled using the snmp-server enable trap command. Notifications are limited to one per second and to one per source MAC and violation reason. Additional violations within a second of a notification being sent will not result in further notifications. Default: disabled.
`link-down`	Shut down the port that received the packet. Default: disabled.

Default When the switch detects an ARP security violation, it drops the packet. By default, it does not perform any other violation actions.

Mode Interface Configuration (switch ports, static or dynamic aggregated links)

Usage notes When the switch detects an ARP security violation on an untrusted port in a VLAN that has ARP security enabled, it drops the packet. This command sets the switch to perform additional actions in response to ARP violations.

If a port has been shut down in response to a violation, to bring it back up again after any issues have been resolved, use the shutdown command.

Example To send SNMP notifications for ARP security violations on ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap dhcpsnooping
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# arp security violation trap
```

Related commands

arp security

show arp security interface

show arp security statistics

show log

snmp-server enable trap

clear arp security statistics

Overview Use this command to clear ARP security statistics for the specified ports, or for all ports.

Syntax

```
clear arp security statistics [interface <port-list>]
```

Parameter	Description
<port-list>	The ports to clear statistics for. If no ports are specified, statistics are cleared for all ports. The ports may be switch ports, or static or dynamic link aggregators.

Mode Privileged Exec

Example To clear statistics for ARP security on interface port1.0.1, use the command:

```
awplus# clear arp security statistics interface port1.0.1
```

Related commands

arp security violation

show arp security

show arp security statistics

clear ip dhcp snooping binding

Overview Use this command to remove one or more DHCP Snooping dynamic entries from the DHCP Snooping binding database. If no options are specified, all entries are removed from the database.

CAUTION: If you remove entries from the database for current clients, they will lose IP connectivity until they request and receive a new DHCP lease. If you clear all entries, all clients connected to untrusted ports will lose connectivity.

Syntax

```
clear ip dhcp snooping binding [<ipaddr>] [interface
<port-list>] [vlan <vid-list>]
```

Parameter	Description
<ipaddr>	Remove the entry for this client IP address.
<port-list>	Remove all entries for these ports. The port list may contain switch ports, and static or dynamic link aggregators (channel groups).
<vid-list>	Remove all entries associated with these VLANs.

Mode Privileged Exec

Usage This command removes dynamic entries from the database. Note that dynamic entries can also be deleted by using the **no** variant of the ip dhcp snooping binding command.

Dynamic entries can individually restored by using the ip dhcp snooping binding command.

To remove static entries, use the **no** variant of the ip source binding command.

Example To remove a dynamic lease entry from the DHCP snooping database for a client with the IP address 192.168.1.2, use the command:

```
awplus# clear ip dhcp snooping binding 192.168.1.2
```

Related commands

ip dhcp snooping binding

ip source binding

show ip dhcp snooping binding

clear ip dhcp snooping statistics

Overview Use this command to clear DHCP snooping statistics for the specified ports, or for all ports.

Syntax

```
clear ip dhcp snooping statistics [interface <port-list>]
```

Parameter	Description
<port-list>	The ports to clear statistics for. If no ports are specified, statistics are cleared for all ports. The port list can contain switch ports, or static or dynamic link aggregators.

Mode Privileged Exec

Example To clear statistics for the DHCP snooping on interface port1.0.1, use the command:

```
awplus# clear ip dhcp snooping statistics interface port1.0.1
```

Related commands

clear arp security statistics

show ip dhcp snooping

show ip dhcp snooping statistics

debug arp security

Overview Use this command to enable ARP security debugging.

Use the **no** variant of this command to disable debugging for ARP security.

Syntax

```
debug arp security
no debug arp security
```

Default Disabled

Mode Privileged Exec

Example To enable ARP security debugging, use the commands:

```
awplus# debug arp security
```

Related commands show debugging arp security

show log

terminal monitor

debug ip dhcp snooping

Overview Use this command to enable the specified types of debugging for DHCP snooping.

Use the **no** variant of this command to disable the specified types of debugging.

Syntax

```
debug ip dhcp snooping {all|acl|db|packet [detail]}
no debug ip dhcp snooping {all|acl|db|packet [detail]}
```

Parameter	Description
`all`	All DHCP snooping debug.
`acl`	DHCP snooping access list debug.
`db`	DHCP snooping binding database debug.
`packet`	DHCP snooping packet debug. For the **no** variant of this command, this option also disables detailed packet debug, if it was enabled.
`detail`	Detailed packet debug.

Default Disabled

Mode Privileged Exec

Example To enable access list debugging for DHCP snooping, use the commands:

```
awplus# debug ip dhcp snooping acl
```

Related commands

debug arp security

show debugging ip dhcp snooping

show log

terminal monitor

ip dhcp snooping

Overview Use this command to enable DHCP snooping on one or more VLANs.

Use the **no** variant of this command to disable DHCP snooping on the VLANs.

Syntax

```
ip dhcp snooping
no ip dhcp snooping
```

Default DHCP snooping is disabled on VLANs by default.

Mode Interface Configuration (VLANs)

Usage notes

Enabling DHCP snooping

For DHCP snooping to operate on a VLAN, you must:

- enable the service on the switch by using the service dhcp-snooping command, and
- enable DHCP snooping on the particular VLAN by using the ip dhcp snooping command, and
- if there is an external DHCP server, configure the port connected to the server as a trusted port, by using the ip dhcp snooping trust command

Disabling DHCP snooping

Use **no service dhcp-snooping** to disable DHCP snooping.

Disabling DHCP snooping removes all DHCP snooping configuration from the running configuration, except for:

- any DHCP snooping maximum bindings settings (ip dhcp snooping max-bindings), and
- any additional DHCP snooping-based ACLs you have created for filtering on untrusted ports.

You must remove any such additional DHCP snooping-based ACLs, using the **no access-group** command. This is because these ACLs block all traffic except for traffic that matches DHCP snooping entries. Once you have disabled DHCP snooping, these ACLs will block all traffic. Note that if you disable DHCP snooping on particular VLANs (using the **no ip dhcp snooping** command), you need to make sure you remove any such additional ACLs that apply to those VLANs.

If you re-enable the service, the switch repopulates the DHCP snooping database from the dynamic lease entries in the database backup file (see the ip dhcp snooping database command). It also updates the lease expiry times.

Examples To enable DHCP snooping on VLANs 2 to 4, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ip dhcp snooping
```

To disable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no ip dhcp snooping
```

Related commands

ip dhcp snooping trust

service dhcp-snooping

show ip dhcp snooping

ip dhcp snooping agent-option

Overview Use this command to enable DHCP Relay Agent Option 82 information insertion on the switch. When this is enabled, the switch:

- inserts DHCP Relay Agent Option 82 information into DHCP packets that it receives on untrusted ports
- removes DHCP Relay Agent Option 82 information from DHCP packets that it sends to untrusted ports.

Use the **no** variant of this command to disable DHCP Relay Agent Option 82 insertion.

Syntax

```
ip dhcp snooping agent-option
no ip dhcp snooping agent-option
```

Default DHCP Relay Agent Option 82 insertion is enabled by default when DHCP snooping is enabled.

Mode Global Configuration

Usage notes DHCP snooping must also be enabled on the switch (service dhcp-snooping command), and on the VLANs (ip dhcp snooping command).

If a subscriber ID is configured for the port (ip dhcp snooping subscriber-id command), the switch includes this in the DHCP Relay Agent Option 82 information it inserts into DHCP packets received on the port.

Example To disable DHCP Relay Agent Option 82 on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping agent-option
```

Related commands

ip dhcp snooping

ip dhcp snooping agent-option allow-untrusted

ip dhcp snooping subscriber-id

service dhcp-snooping

show ip dhcp snooping

ip dhcp snooping agent-option allow-untrusted

Overview Use this command to enable DHCP Relay Agent Option 82 information reception on untrusted ports. When this is enabled, the switch accepts incoming DHCP packets that contain DHCP Relay Agent Option 82 information on untrusted ports.

Use the **no** variant of this command to disable DHCP Relay Agent Option 82 information reception on untrusted ports.

Syntax

```
ip dhcp snooping agent-option allow-untrusted
no ip dhcp snooping agent-option allow-untrusted
```

Default Disabled

Mode Global Configuration

Usage notes If the switch is connected via untrusted ports to edge switches that insert DHCP Relay Agent Option 82 information into DHCP packets, you may need to allow these DHCP packets through the untrusted ports, by using this command.

When this is disabled (default), the switch treats incoming DHCP packets on untrusted ports that contain DHCP Relay Agent Option 82 information as DHCP snooping violations: it drops them and applies any violation action specified by the ip dhcp snooping violation command. The switch stores statistics for packets dropped; to display these statistics, use the show ip dhcp snooping statistics command.

Example To enable DHCP snooping Option 82 information reception on untrusted ports, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping agent-option allow-untrusted
```

Related commands

ip dhcp snooping agent-option

ip dhcp snooping violation

show ip dhcp snooping

show ip dhcp snooping statistics

ip dhcp snooping agent-option circuit-id vlantriplet

Overview Use this command to specify the Circuit ID sub-option of the DHCP Relay Agent Option 82 field as the VLAN ID and port number. The Circuit ID specifies the switch port and VLAN ID that the client-originated DHCP packet was received on.

Use the **no** variant of this command to set the Circuit ID to the default, the VLAN ID and Ifindex (interface number).

Syntax

```
ip dhcp snooping agent-option circuit-id vlantriplet
no ip dhcp snooping agent-option circuit-id
```

Default By default, the Circuit ID is the VLAN ID and Ifindex (interface number).

Mode Interface Configuration for a VLAN interface.

Usage The Circuit ID sub-option is included in the DHCP Relay Agent Option 82 field of forwarded client DHCP packets:

- DHCP snooping Option 82 information insertion is enabled (ip dhcp snooping agent-option command; enabled by default), and
- DHCP snooping is enabled on the switch (service dhcp-snooping) and on the VLAN to which the port belongs (ip dhcp snooping)

Examples To set the Circuit ID to `vlantriplet` for client DHCP packets received on `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp snooping agent-option circuit-id
vlantriplet
```

To return the Circuit ID format to the default for `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp snooping agent-option circuit-id
```

Related commands

ip dhcp snooping agent-option

ip dhcp snooping agent-option remote-id

show ip dhcp snooping

show ip dhcp snooping agent-option

ip dhcp snooping agent-option remote-id

Overview Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field. The Remote ID identifies the device that inserted the Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the switch's MAC address.

Use the **no** variant of this command to set the Remote ID to the default, the switch's MAC address.

Syntax

```
ip dhcp snooping agent-option remote-id <remote-id>
no ip dhcp snooping agent-option remote-id
```

Parameter	Description
<remote-id>	An alphanumeric (ASCII) string, 1 to 63 characters in length. If the Remote ID contains spaces, it must be enclosed in double quotes. Wildcards are not allowed.

Default The Remote ID is set to the switch's MAC address by default.

Mode Interface Configuration for a VLAN interface.

Usage The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of forwarded client DHCP packets:

- DHCP snooping Option 82 information insertion is enabled (ip dhcp snooping agent-option command; enabled by default), and
- DHCP snooping is enabled on the switch (service dhcp-snooping) and on the VLAN to which the port belongs (ip dhcp snooping)

Examples To set the Remote ID to `myid` for client DHCP packets received on `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp snooping agent-option remote-id myid
```

To return the Remote ID format to the default for `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp snooping agent-option remote-id
```

Related commands

ip dhcp snooping agent-option

ip dhcp snooping agent-option circuit-id vlantriplet

show ip dhcp snooping

show ip dhcp snooping agent-option

ip dhcp snooping binding

Overview Use this command to manually add a dynamic-like entry (with an expiry time) to the DHCP snooping database. Once added to the database, this entry is treated as a dynamic entry, and is stored in the DHCP snooping database backup file. This command is not stored in the switch's running configuration.

Use the **no** variant of this command to delete a dynamic entry for an IP address from the DHCP snooping database, or to delete all dynamic entries from the database.

CAUTION: If you remove entries from the database for current clients, they will lose IP connectivity until they request and receive a new DHCP lease. If you clear all entries, all clients connected to untrusted ports will lose connectivity.

Syntax

```
ip dhcp snooping binding <ipaddr> [<macaddr>] vlan <vid>
interface <port> expiry <expiry-time>
```

```
no ip dhcp snooping binding [<ipaddr>]
```

Parameter	Description
<ipaddr>	Client's IP address.
<macaddr>	Client's MAC address in HHHH.HHHH.HHHH format.
<vid>	The VLAN ID for the entry, in the range 1 to 4094.
<port>	The port the client is connected to. The port can be a switch port, or a static or dynamic link aggregation (channel group).
<expiry-time>	The expiry time for the entry, in the range 5 to 2147483647 seconds.

Mode Privileged Exec

Usage notes Note that dynamic entries can also be deleted from the DHCP snooping database by using the clear ip dhcp snooping binding command.

To add or remove static entries from the database, use the ip source binding command.

Example To restore an entry in the DHCP snooping database for a DHCP client with the IP address 192.168.1.2, MAC address 0001.0002.0003, on port1.0.6 of vlan6, and with an expiry time of 1 hour, use the commands:

```
awplus# ip dhcp snooping binding 192.168.1.2 0001.0002.0003
vlan 6 interface port1.0.6 expiry 3600
```

Related commands

clear ip dhcp snooping binding

ip source binding

show ip dhcp snooping binding

ip dhcp snooping database

Overview Use this command to set the location of the file to which the dynamic entries in the DHCP snooping database are written. This file provides a backup for the DHCP snooping database.

Use the **no** variant of this command to set the database location back to the default, **nvs**.

Syntax

```
ip dhcp snooping database {nvs|flash|usb}
no ip dhcp snooping database
```

Parameter	Description
`nvs`	The switch checks the database and writes the file to non-volatile storage (NVS) on the switch at 2 second intervals if it has changed.
`flash`	The switch checks the database and writes the file to Flash memory on the switch at 60 second intervals if it has changed.
`usb`	The switch checks the database and writes the file to a USB storage device installed in the switch at 2 second intervals if it has changed.

Default nvs

Mode Global Configuration

Usage notes If the location of the backup file is changed by using this command, a new file is created in the new location, and the old version of the file remains in the old location. This can be removed if necessary (hidden file: **.dhcp.dsn.gz**).

Example To set the location of the DHCP snooping database to Flash memory, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping database flash
```

Related commands show ip dhcp snooping

ip dhcp snooping delete-by-client

Overview Use this command to set the switch to remove a dynamic entry from the DHCP snooping database when it receives a valid DHCP release message with matching IP address, VLAN ID, and client hardware address on an untrusted port, and to discard release messages that do not match an entry in the database.

Use the **no** variant of this command to set the switch to forward DHCP release messages received on untrusted ports without removing any entries from the database.

Syntax

```
ip dhcp snooping delete-by-client
no ip dhcp snooping delete-by-client
```

Default Enabled: by default, DHCP lease entries are deleted from the DHCP snooping database when matching DHCP release messages are received.

Mode Global Configuration

Usage DHCP clients send a release message when they no longer wish to use the IP address they have been allocated by a DHCP server. Use this command to enable DHCP snooping to use the information in these messages to remove entries from its database immediately. Use the **no** variant of this command to ignore these release messages. Lease entries corresponding to ignored DHCP release messages eventually time out when the lease expires.

Examples To set the switch to delete DHCP snooping lease entries from the DHCP snooping database when a matching release message is received, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping delete-by-client
```

To set the switch to forward and ignore the content of any DHCP release messages it receives, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping delete-by-client
```

Related commands show ip dhcp snooping

ip dhcp snooping delete-by-linkdown

Overview Use this command to set the switch to remove a dynamic entry from the DHCP snooping database when its port goes down. If the port is part of an aggregated link, the entries in the database are only deleted if all the ports in the aggregated link are down.

Use the **no** variant of this command to set the switch not to delete entries when ports go down.

Syntax

```
ip dhcp snooping delete-by-linkdown
no ip dhcp snooping delete-by-linkdown
```

Default Disabled: by default DHCP Snooping bindings are not deleted when an interface goes down.

Mode Global Configuration

Examples To set the switch to delete DHCP snooping lease entries from the DHCP snooping database when links go down, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping delete-by-linkdown
```

To set the switch not to delete DHCP snooping lease entries from the DHCP snooping database when links go down, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping delete-by-linkdown
```

Related commands show ip dhcp snooping

ip dhcp snooping max-bindings

Overview Use this command to set the maximum number of DHCP lease entries that can be stored in the DHCP snooping database for each of the ports. Once this limit has been reached, no further DHCP lease allocations made to devices on the port are stored in the database.

Use the **no** variant of this command to reset the maximum to the default, 1.

Syntax

```
ip dhcp snooping max-bindings <0-520>
no ip dhcp snooping max-bindings
```

Parameter	Description
<0-520>	The maximum number of bindings that will be stored for the port in the DHCP snooping binding database. If 0 is specified, no entries will be stored in the database for the port.

Default The default for maximum bindings is 1.

Mode Interface Configuration (port)

Usage notes The maximum number of leases cannot be changed for a port while there are DHCP snooping Access Control Lists (ACL) associated with the port. Before using this command, remove any DHCP snooping ACLs associated with the ports. To display ACLs used for DHCP snooping, use the show ip dhcp snooping acl command.

In general, the default (1) will work well on an edge port with a single directly connected DHCP client. If the port is on an aggregation switch that is connected to an edge switch with multiple DHCP clients connected through it, then use this command to increase the number of lease entries for the port.

If there are multiple VLANs configured on the port, the limit is shared between all the VLANs on this port. For example, the default only allows one lease to be stored for one VLAN. To allow connectivity for the other VLANs, use this command to increase the number of lease entries for the port.

Example To set the maximum number of bindings to be stored in the DHCP snooping database to 10 per port for ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# ip dhcp snooping max-bindings 10
```

Related commands

access-group

show ip dhcp snooping acl

show ip dhcp snooping interface

ip dhcp snooping subscriber-id

Overview Use this command to set a Subscriber ID for the ports.

Use the **no** variant of this command to remove Subscriber IDs from the ports.

Syntax

```
ip dhcp snooping subscriber-id [<sub-id>]
no ip dhcp snooping subscriber-id
```

Parameter	Description
<sub-id>	The Subscriber ID; an alphanumeric (ASCII) string 1 to 50 characters in length. If the Subscriber ID contains spaces, it must be enclosed in double quotes. Wildcards are not allowed.

Default No Subscriber ID.

Mode Interface Configuration (port)

Usage notes The Subscriber ID sub-option is included in the DHCP Relay Agent Option 82 field of client DHCP packets forwarded from a port if:

- a Subscriber ID is specified for the port using this command, and
- DHCP snooping Option 82 information insertion is enabled (ip dhcp snooping agent-option command; enabled by default), and
- DHCP snooping is enabled on the switch (service dhcp-snooping) and on the VLAN to which the port belongs (ip dhcp snooping)

Examples To set the Subscriber ID for port 1.0.3 to **room_534**, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# ip dhcp snooping subscriber-id room_534
```

To remove the Subscriber ID from port 1.0.3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no ip dhcp snooping subscriber-id
```

Related commands ip dhcp snooping agent-option

show ip dhcp snooping interface

ip dhcp snooping trust

Overview Use this command to set the ports to be DHCP snooping trusted ports.

Use the **no** variant of this command to return the ports to their default as untrusted ports.

Syntax

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

Default All ports are untrusted by default.

Mode Interface Configuration (port)

Usage notes Typically, ports connecting the switch to trusted elements in the network (towards the core) are set as trusted ports, while ports connecting untrusted network elements are set as untrusted. Configure ports connected to DHCP servers as trusted ports.

Example To set switch ports 1.0.1 and 1.0.2 to be trusted ports, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# ip dhcp snooping trust
```

Related commands show ip dhcp snooping interface

ip dhcp snooping verify mac-address

Overview Use this command to verify that the source MAC address and client hardware address match in DHCP packets received on untrusted ports.

Use the **no** variant of this command to disable MAC address verification.

Syntax

```
ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address
```

Default Enabled—source MAC addresses are verified by default.

Mode Global Configuration

Usage When MAC address verification is enabled, the switch treats DHCP packets with source MAC address and client hardware address that do not match as DHCP snooping violations: it drops them and applies any other violation action specified by the ip dhcp snooping violation command. To bring the port back up again after any issues have been resolved, use the shutdown command.

Example To disable MAC address verification on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping verify mac-address
```

Related commands

ip dhcp snooping violation

show ip dhcp snooping

show ip dhcp snooping statistics

ip dhcp snooping violation

Overview Use this command to specify the action the switch will take when it detects a DHCP snooping violation by a DHCP packet on the ports.

Use the **no** variant of this command to disable the specified violation actions, or all violation actions.

Syntax

```
ip dhcp snooping violation {log|trap|link-down} ...
no ip dhcp snooping violation [{log|trap|link-down} ...]
```

Parameter	Description
`log`	Generate a log message. To display these messages, use the show log command. Default: disabled.
`trap`	Generate an SNMP notification (trap). To send SNMP notifications, SNMP must also be configured, and DHCP snooping notifications must be enabled using the snmp-server enable trap command. Notifications are limited to one per second and to one per source MAC and violation reason. Default: disabled.
`link-down`	Set the port status to link-down. Default: disabled.

Default By default, DHCP packets that violate DHCP snooping are dropped, but no other violation action is taken.

Mode Interface Configuration (port)

Usage notes If a port has been shut down in response to a violation, to bring it back up again after any issues have been resolved, use the shutdown command.

IP packets dropped by DHCP snooping filters do not result in other DHCP snooping violation actions.

Example To set the switch to send an SNMP notification and set the link status to link-down if it detects a DHCP snooping violation on switch ports 1.0.1 to 1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap dhcpsnooping
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# ip dhcp snooping violation trap link-down
```

Related commands

show ip dhcp snooping interface

show log

snmp-server enable trap

ip source binding

Overview Use this command to add or replace a static entry in the DHCP snooping database.

Use the **no** variant of this command to delete the specified static entry or all static entries from the database.

Syntax

```
ip source binding <ipaddr> [<macaddr>] vlan <vid> interface
<port>
```

```
no ip source binding [<ipaddr>]
```

Parameter	Description
<ipaddr>	Client's IP address. If there is already an entry in the DHCP snooping database for this IP address, then this command replaces it with the new entry.
<macaddr>	Client's MAC address in HHHH.HHHH.HHHH format.
<vid>	The VLAN ID associated with the entry.
<port>	The port the client is connected to.

Mode Global Configuration

Usage notes This command removes static entries from the database.

To remove dynamic entries, use the clear ip dhcp snooping binding command or the **no** variant of the ip dhcp snooping binding command.

Examples To add a static entry to the DHCP snooping database for a client with the IP address 192.168.1.2, MAC address 0001.0002.0003, on port1.0.6 of vlan6, use the command:

```
awplus# configure terminal
awplus(config)# ip source binding 192.168.1.2 0001.0002.0003
vlan 6 interface port1.0.6
```

To remove the static entry for IP address 192.168.1.2 from the database, use the commands:

```
awplus# configure terminal
awplus(config)# no ip source binding 192.168.1.2
```

To remove all static entries from the database, use the commands:

```
awplus# configure terminal
awplus(config)# no ip source binding
```

Related commands

clear ip dhcp snooping binding

ip dhcp snooping binding

show ip dhcp snooping binding

show ip source binding

service dhcp-snooping

Overview Use the **service dhcp-snooping** command to enable the DHCP snooping service globally on the switch. As well, you need to enable it on the desired VLANs, using the ip dhcp snooping command. The switch creates a global DHCP snooping Access Control list (ACL) the first time you use the ip dhcp snooping command, to send DHCP packets to the CPU for processing. Note that the switch will forward all DHCP traffic to the CPU, no matter what VLAN it belongs to.

Alternatively, you can use the **service dhcp-snooping per-vlan** command instead of the **service dhcp-snooping** command. This option only creates an ACL for the VLANs that you configure with the ip dhcp snooping command. This limits the amount of DHCP traffic that is forwarded to the CPU. However, using this option creates an ACL for each VLAN that DHCP snooping is enabled on, so it is most suitable if you have a small number of VLANs. Use the **show platform classifier statistics utilization brief** command to see the number of ACLs available for your switch.

Use the **no** variant of this command to disable the DHCP snooping service on the switch.

Syntax

```
service dhcp-snooping
service dhcp-snooping per-vlan
no service dhcp-snooping
```

Parameter	Description
`per-vlan`	This optional parameter only enables DHCP snooping for the VLANs configured using the command ip dhcp snooping. Using this option creates an ACL entry for only the VLANs that DHCP snooping is enabled on. This limits the DHCP traffic forwarded to the CPU.

Default Disabled

Mode Global Configuration

Usage notes

Enabling DHCP snooping

For DHCP snooping to operate on a VLAN, you must:

- enable the service on the switch by using this command, and
- enable DHCP snooping on the particular VLAN by using the ip dhcp snooping command, and
- if there is an external DHCP server, configure the port connected to the server as a trusted port, by using the ip dhcp snooping trust command

Disabling DHCP snooping

Use **no service dhcp-snooping** to disable DHCP snooping.

Disabling DHCP snooping removes all DHCP snooping configuration from the running configuration, except for:

- any DHCP snooping maximum bindings settings (ip dhcp snooping max-bindings), and
- any additional DHCP snooping-based ACLs you have created for filtering on untrusted ports.

You must remove any such additional DHCP snooping-based ACLs, using the **no access-group** command. This is because these ACLs block all traffic except for traffic that matches DHCP snooping entries. Once you have disabled DHCP snooping, these ACLs will block all traffic. Note that if you disable DHCP snooping on particular VLANs (using the **no ip dhcp snooping** command), you need to make sure you remove any such additional ACLs that apply to those VLANs.

If you re-enable the service, the switch repopulates the DHCP snooping database from the dynamic lease entries in the database backup file (see the ip dhcp snooping database command). It also updates the lease expiry times.

Examples

To enable the DHCP snooping service on only the VLANs that have DHCP snooping enabled, use the command:

```
awplus# configure terminal
awplus(config)# service dhcp-snooping
```

To disable the DHCP snooping service on the switch, use the command:

```
awplus# configure terminal
awplus(config)# no service dhcp-snooping
```

Related commands

access-group

ip dhcp snooping

ip dhcp snooping database

ip dhcp snooping max-bindings

show ip dhcp snooping

Command changes

Version 5.4.9-2.1: **per-vlan** parameter added for IE510, IE340, IE300, SBx908 GEN2, x950, x930, x510.

show arp security

Overview Use this command to display ARP security configuration.

Syntax

```
show arp security
```

Mode User Exec and Privileged Exec

Example To display ARP security configuration on the switch use the command:

```
awplus# show arp security
```

Table 1: Example output from the **show arp security** command

```
awplus# show arp security

ARP Security Information:
  Total VLANs enabled ..... 2
  Total VLANs disabled ..... 11
  vlan1 ..... Disabled
  vlan2 ..... Disabled
  vlan3 ..... Disabled
  vlan4 ..... Disabled
  vlan5 ..... Disabled
  vlan100 ..... Disabled
  vlan101 ..... Disabled
  vlan102 ..... Disabled
  vlan103 ..... Disabled
  vlan104 ..... Disabled
  vlan105 ..... Enabled
  vlan1000 ..... Disabled
  vlan1001 ..... Enabled
```

Table 2: Parameters in the output from the **show arp security** command

Parameter	Description
`Total VLANs enabled`	The number of VLANs that have ARP security enabled.
`Total VLANs disabled`	The number of VLANs that have ARP security disabled.

Related commands

arp security

show arp security interface

show arp security statistics

show arp security interface

Overview Use this command to display ARP security configuration for the specified ports or all ports.

Syntax `show arp security interface [<port-list>]`

Parameter	Description
<port-list>	The ports to display ARP security information about. The port list can include switch ports, and static or dynamic aggregated links.

Mode User Exec and Privileged Exec

Example To display ARP security configuration for ports, use the command:

```
awplus# show arp security interface
```

Table 3: Example output from the **show arp security interface** command

```
awplus#show arp security interface

Arp Security Port Status and Configuration:

  Port: Provisioned ports marked with brackets, e.g. (portx.y.z)
  KEY:  LG = Log
        TR = Trap
        LD = Link down

Port         Action
------------------------------
port1.0.1    -- -- --
port1.0.2    -- -- --
port1.0.3    LG TR LD
port1.0.4    LG -- --
port1.0.5    LG -- --
port1.0.6    LG TR --
port1.0.7    LG -- LD
...
```

Table 4: Parameters in the output from the **show arp security interface** command

Parameter	Description
`Action`	The action the switch takes when it detects an ARP security violation on the port.
`Port`	The port. Parentheses indicate that ports are configured for provisioning.
`LG, Log`	Generate a log message
`TR, Trap`	Generate an SNMP notification (trap).
`LD, Link down`	Shut down the link.

Related commands

arp security violation

show arp security

show arp security statistics

show log

snmp-server enable trap

show arp security statistics

Overview Use this command to display ARP security statistics for the specified ports or all ports.

Syntax `show arp security statistics [detail] [interface <port-list>]`

Parameter	Description
`detail`	Display detailed statistics.
`interface <port-list>`	Display statistics for the specified ports. The port list can include switch ports, and static or dynamic aggregated links

Mode User Exec and Privileged Exec

Example To display the brief statistics for the ARP security, use the command:

```
awplus# show arp security statistics
```

Table 5: Example output from the **show arp security statistics** command

```
awplus# show arp security statistics

DHCP Snooping ARP Security Statistics:
              In          In
 Interface    Packets     Discards
---------------------------------
 port1.0.3    20          20
 port1.0.4    30          30
 port1.0.12   120         0
```

Table 6: Parameters in the output from the **show arp security statistics** command

Parameter	Description
`Interface`	A port name. Parentheses indicate that ports are configured for provisioning.
`In Packets`	The total number of incoming ARP packets that are processed by DHCP Snooping ARP Security
`In Discards`	The total number of ARP packets that are dropped by DHCP Snooping ARP Security.

Table 7: Example output from the **show arp security statistics detail** command

```
awplus#show arp security statistics detail

DHCP Snooping ARP Security Statistics:
Interface ..................... port1.0.3
  In Packets .................. 20
  In Discards ................. 20
    No Lease .................. 20
    Bad Vlan .................. 0
    Bad Port .................. 0
    Source Ip Not Allocated .... 0
Interface ..................... port1.0.4
  In Packets .................. 30
  In Discards ................. 30
    No Lease .................. 30
    Bad Vlan .................. 0
    Bad Port .................. 0
    Source Ip Not Allocated .... 0
Interface ..................... port1.0.12
  In Packets .................. 120
  In Discards ................. 0
    No Lease .................. 0
    Bad Vlan .................. 0
    Bad Port .................. 0
    Source Ip Not Allocated .... 0
```

Related commands

arp security

arp security violation

clear arp security statistics

show arp security

show arp security interface

show log

show debugging arp security

Overview Use this command to display the ARP security debugging configuration.

Syntax

```
show debugging arp security
```

Mode User and Privileged Exec

Example To display the debugging settings for ARP security on the switch, use the command:

```
awplus# show debugging arp security
```

Table 8: Example output from the **show debugging arp security** command

```
awplus# show debugging arp security

ARP Security debugging status:
  ARP Security debugging is off
```

Related commands

arp security violation

debug arp security

show debugging ip dhcp snooping

Overview Use this command to display the DHCP snooping debugging configuration.

Syntax

```
show debugging ip dhcp snooping
```

Mode User Exec and Privileged Exec

Example To display the DHCP snooping debugging configuration, use the command:

```
awplus# show debugging ip dhcp snooping
```

Table 9: Example output from the **show debugging ip dhcp snooping** command

```
awplus# show debugging ip dhcp snooping

DHCP snooping debugging status:
  DHCP snooping debugging is off
  DHCP snooping all debugging is off
  DHCP snooping acl debugging is off
  DHCP snooping binding DB debugging is off
  DHCP snooping packet debugging is off
  DHCP snooping detailed packet debugging is off
```

Related commands

debug ip dhcp snooping

show log

show ip dhcp snooping

Overview Use this command to display DHCP snooping global configuration on the switch.

Syntax

```
show ip dhcp snooping
```

Mode User Exec and Privileged Exec

Example To display global DHCP snooping configuration on the switch, use the command:

```
awplus# show ip dhcp snooping
```

Table 50-1: Example output from **show ip dhcp snooping**

```
DHCP Snooping Information:
  DHCP Snooping service ............. Enabled

Option 82 insertion ............... Enabled

Option 82 on untrusted ports ...... Not allowed
  Binding delete by client .......... Disabled
  Binding delete by link down ....... Disabled
  Verify MAC address ................ Disabled
  SNMP DHCP Snooping trap ........... Disabled

DHCP Snooping database:
  Database location ................. nvs  Number of entries in
database ..... 2

DHCP Snooping VLANs:
  Total VLANs enabled ............... 1
  Total VLANs disabled .............. 9
  vlan1 ............... Enabled
  vlan2 ............... Disabled
  vlan3 ............... Disabled
  vlan4 ............... Disabled
  vlan5 ............... Disabled
  vlan100 ............. Disabled
  vlan101 ............. Disabled
  vlan105 ............. Disabled
  vlan1000 ............ Disabled
  vlan1001 ............ Disabled
```

Related commands

service dhcp-snooping

show arp security

show ip dhcp snooping acl

show ip dhcp snooping agent-option

show ip dhcp snooping binding

show ip dhcp snooping interface

show ip dhcp snooping acl

Overview Use this command to display information about the Access Control Lists (ACL) that are using the DHCP snooping database.

Syntax

```
show ip dhcp snooping acl
show ip dhcp snooping acl [detail|hardware] [interface
[<interface-list>]]
```

Parameter	Description
`detail`	Detailed DHCP Snooping ACL information.
`hardware`	DHCP Snooping hardware ACL information.
`interface`	ACL Interface information.
<interface-list>	The interfaces to display information about.

Mode User Exec and Privileged Exec

Example To display DHCP snooping ACL information, use the command:

```
awplus# show ip dhcp snooping acl
```

Table 51: Example output from the **show ip dhcp snooping acl** command

```
awplus#show ip dhcp snooping acl

DHCP Snooping Based Filters Summary:

                       Maximum   Template  Attached
Interface    Bindings  Bindings  Filters   Hardware Filters
-------------------------------------------------------------
 port1.0.1   1         520       0         0
 port1.0.2   1         3         2         6
 port1.0.3   1         2         4         8
 port1.0.4   1         2         7         14
 port1.0.5   0         2         6         12
 port1.0.6   0         1         0         0
 port1.0.7   0         1         0         0
 port1.0.8   0         1         0         0
 port1.0.9   0         1         0         0
 port1.0.10  0         1         0         0
 port1.0.11  0         1         0         0
 port1.0.12  0         1         0         0
(port2.0.1 ) 0         520       0         0
(port2.0.2 ) 0         1         0         0
```

To display DHCP snooping hardware ACL information, use the command:

```
awplus# show ip dhcp snooping acl hardware
```

Table 52: Example output from the **show ip dhcp snooping acl hardware** command

```
awplus#show ip dhcp snooping acl hardware

DHCP Snooping Based Filters in Hardware:

Interface    Access-list(/ClassMap)        Source IP         Source MAC
-------------------------------------------------------------------------
 port1.0.2   dhcpsn1                       10.10.10.10       aaaa.bbbb.cccc
 port1.0.2   dhcpsn1                       20.20.20.20       0000.aaaa.bbbb
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 30.30.30.30       aaaa.bbbb.dddd
 port1.0.3   dhcpsn2/cmap1                 40.40.40.40       0000.aaaa.cccc
 port1.0.3   dhcpsn2/cmap1                 50.50.50.50       0000.aaaa.dddd
 port1.0.3   dhcpsn2/cmap1                 60.60.60.60       0000.aaaa.eeee
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.4   dhcpsn3/cmap2                 70.70.70.70
 port1.0.4   dhcpsn3/cmap2                 80.80.80.80
 port1.0.4   dhcpsn2/cmap1                 70.70.70.70
 port1.0.4   dhcpsn2/cmap1                 80.80.80.80
 port1.0.4   dhcpsn1                       70.70.70.70
 port1.0.4   dhcpsn1                       80.80.80.80
```

To display detailed DHCP snooping ACL information for port 1.0.4, use the command:

```
awplus# show ip dhcp snooping acl detail interface port1.0.4
```

Table 53: Example output from the **show ip dhcp snooping acl detail interface** command

```
awplus#show ip dhcp snooping acl detail interface port1.0.4

DHCP Snooping Based Filters Information:

 port1.0.4 : Maximum Bindings ........... 2
 port1.0.4 : Template filters ........... 7
 port1.0.4 : Attached hardware filters .. 14
 port1.0.4 : Current bindings ........... 1, 1 free
 port1.0.4    Client 1 ................. 120.120.120.120
 port1.0.4 : Templates: cheese (via class-map: cmap2)
 port1.0.4 :  10 permit ip dhcpsnooping 100.0.0.0/8
 port1.0.4 : Template: dhcpsn2 (via class-map: cmap1)
 port1.0.4 :  10 permit ip dhcpsnooping any
 port1.0.4 :  20 permit ip dhcpsnooping 10.0.0.0/8
 port1.0.4 :  30 permit ip dhcpsnooping 20.0.0.0/8
 port1.0.4 :  40 permit ip dhcpsnooping 30.0.0.0/8
 port1.0.4 : Template: dhcpsn1 (via access-group)
 port1.0.4 :  10 permit ip dhcpsnooping any mac dhcpsnooping abcd.0000.0000 00
 00.ffff.ffff
 port1.0.4 : 20 permit ip dhcpsnooping any
```

Related commands

access-list hardware (named hardware ACL)

show access-list (IPv4 Hardware ACLs)

show ip dhcp snooping agent-option

Overview Use this command to display DHCP snooping Option 82 information for all interfaces, a specific interface or a range of interfaces.

Syntax `show ip dhcp snooping agent-option [interface <interface-list>]`

Parameter	Description
`interface`	Specify the interface.
`<interface-list>`	The name of the interface or interfaces.

Mode User Exec and Privileged Exec

Examples To display DHCP snooping Option 82 information for all interfaces, use the command:

```
awplus# show ip dhcp snooping agent-option
```

To display DHCP snooping Option 82 information for vlan1, use the command:

```
awplus# show ip dhcp snooping agent-option interface vlan1
```

To display DHCP snooping Option 82 information for port1.0.1, use the command:

```
awplus# show ip dhcp snooping agent-option interface port1.0.1
```

Output Figure 50-1: Example output from the **show ip dhcp snooping agent-option** command

```
awplus#show ip dhcp snooping agent-option

DHCP Snooping Option 82 Configuration:

  Key:      C Id = Circuit Id Format
            R Id = Remote Id
            S Id = Subscriber Id

  Option 82 insertion ............... Enabled
  Option 82 on untrusted ports ...... Not allowed

------------------------------------------------------------------
 vlan1       C Id = vlanifindex
             R Id = Access-Island-01-M1
 vlan2       C Id = vlantriplet
             R Id = Access-Island-01-M1
 vlan3       C Id = vlantriplet
             R Id = Access-Island-01-M3
 vlan4       C Id = vlantriplet
             R Id = 0000.cd28.074c
 vlan5       C Id = vlantriplet
             R Id = 0000.cd28.074c
 vlan6       C Id = vlantriplet
             R Id = 0000.cd28.074c
 port1.0.1   S Id =
 port1.0.2   S Id =
 port1.0.3   S Id = phone_1
 port1.0.4   S Id =
 port1.0.5   S Id = PC_1
 port1.0.6   S Id = phone_2
```

Related commands

ip dhcp snooping agent-option

ip dhcp snooping agent-option circuit-id vlantriplet

ip dhcp snooping agent-option remote-id

ip dhcp snooping subscriber-id

show ip dhcp snooping

show ip dhcp snooping interface

show ip dhcp snooping binding

Overview Use this command to display all dynamic and static entries in the DHCP snooping binding database.

Syntax

```
show ip dhcp snooping binding
```

Mode User Exec and Privileged Exec

Example To display entries in the DHCP snooping database, use the command:

```
awplus# show ip dhcp snooping binding
```

Table 54: Example output from the **show ip dhcp snooping binding** command

```
awplus# show ip dhcp snooping binding
DHCP Snooping Bindings:

Client           MAC              Server                        Expires
IP Address       Address          IP Address       VLAN  Port   (sec)       Type
-------------------------------------------------------------------------------
1.2.3.4          aaaa.bbbb.cccc   --               7     1.0.6   Infinite   Stat
1.2.3.6          any              --               4077  1.0.6   Infinite   Stat
1.3.4.5          any              --               1     sa1     Infinite   Stat
111.111.100.101  0000.0000.0001   111.112.1.1      1     1.0.6   4076       Dyna
111.111.101.108  0000.0000.0108   111.112.1.1      1     1.0.6   4084       Dyna
111.111.101.109  0000.0000.0109   111.112.1.1      1     1.0.6   4085       Dyna
111.211.100.101  --               --               1     1.0.2   2147483325 Dyna
111.211.100.109  00b0.0000.0009   111.112.111.111  1     1.0.2   21         Dyna
111.211.101.101  00b0.0000.0101   111.112.111.111  1     1.0.2   214        Dyna

Total number of bindings in database: 9
```

Table 55: Parameters in the output from the **show ip dhcp snooping binding** command

Parameter	Description
Client IPAddress	The IP address of the DHCP client.
MAC Address	The MAC address of the DHCP client.
Server IP	The IP address of the DHCP server.
VLAN	The VLAN associated with this entry.
Port	The port the client is connected to.
Expires (sec)	The time in seconds until the lease expires.

Table 55: Parameters in the output from the **show ip dhcp snooping binding** command (cont.)

Parameter	Description
`Type`	The source of the entry: • Dyna: dynamically entered by snooping DHCP traffic, configured by the ip dhcp snooping binding command, or loaded from the database backup file. • Stat: added statically by the ip source binding command
`Total number of bindings in database`	The total number of dynamic and static lease entries in the DHCP snooping database.

Related commands

ip dhcp snooping binding

ip dhcp snooping max-bindings

show ip source binding

show ip dhcp snooping interface

Overview Use this command to display information about DHCP snooping configuration and leases for the specified ports, or all ports.

Syntax `show ip dhcp snooping interface [<port-list>]`

Parameter	Description
<port-list>	The ports to display DHCP snooping configuration information for. If no ports are specified, information for all ports is displayed.

Mode User Exec and Privileged Exec

Example To display DHCP snooping information for all ports, use the command:

```
awplus# show ip dhcp snooping interface
```

Table 56: Example output from the **show ip dhcp snooping interface** command

```
awplus#show ip dhcp snooping interface

DHCP Snooping Port Status and Configuration:

  Port: Provisioned ports marked with brackets, e.g. (portx.y.z)
  Action: LG = Log
          TR = Trap
          LD = Link down

                        Full    Max
 Port         Status     Leases  Leases  Action     Subscriber-ID
-------------------------------------------------------------------------------
 port1.0.1    Untrusted  1       1       LG -- --
 port1.0.2    Untrusted  0       50      LG TR LD   Building 1 Level 1
 port1.0.3    Untrusted  0       50      LG -- --
 port1.0.4    Untrusted  0       50      LG -- --   Building 1 Level 2
 port1.0.5    Untrusted  0       50      LG -- LD   Building 2 Level 1
 port1.0.6    Untrusted  0       1       LG -- --
 port1.0.7    Untrusted  0       1       LG -- --
 port1.0.8    Untrusted  0       1       LG -- --
 port1.0.9    Untrusted  0       1       -- TR --
 port1.0.10   Untrusted  0       1       -- -- LD
 port1.0.11   Trusted    0       1       -- -- --
 port1.0.12   Trusted    0       1       -- -- --
```

Table 57: Parameters in the output from the **show ip dhcp snooping interface** command

Parameter	Description
`Port`	The port interface name.
`Status`	The port status: untrusted (default) or trusted.
`Full Leases`	The number of entries in the DHCP snooping database for the port.
`Max Leases`	The maximum number of entries that can be stored in the database for the port.
`Action`	The DHCP snooping violation actions for the port.
`Subscriber ID`	The subscriber ID for the port. If the subscriber ID is longer than 34 characters, only the first 34 characters are displayed. To display the whole subscriber ID, use the command **show running-config dhcp**.

Related commands

show ip dhcp snooping

show ip dhcp snooping statistics

show running-config dhcp

show ip dhcp snooping statistics

Overview Use this command to display DHCP snooping statistics.

Syntax

```
show ip dhcp snooping statistics [detail] [interface
<interface-list>]
```

Parameter	Description
`detail`	Display detailed statistics.
`interface <interface-list>`	Display statistics for the specified interfaces. The interface list can contain switch ports, static or dynamic link aggregators (channel groups), or VLANs.

Mode User Exec and Privileged Exec

Example To show the current DHCP snooping statistics for all interfaces, use the command:

```
awplus# show ip dhcp snooping statistics
```

Table 58: Example output from the **show ip dhcp snooping statistics** command

```
awplus# show ip dhcp snooping statistics

DHCP Snooping Statistics:
              In BOOTP     In BOOTP     In          In
 Interface    Packets      Requests      Replies    Discards
-------------------------------------------------------------
 vlan1        444          386           58           223
 port1.0.1    386          386           0            223
 port1.0.2    0            0             0            0
 port1.0.3    0            0             0            0
 port1.0.4    0            0             0            0
 port1.0.5    0            0             0            0
 port1.0.6    58           0             58           0
```

Table 59: Example output from the **show ip dhcp snooping statistics detail** command

```
awplus# show ip dhcp snooping statistics detail

DHCP Snooping Statistics:
Interface ....................................... port1.0.1, All counters 0
Interface ....................................... port1.0.2, All counters 0
Interface ....................................... port1.0.3, All counters 0
Interface ....................................... port1.0.4
  In Packets ..................................... 50
    In BOOTP Requests ............................ 25
    In BOOTP Replies ............................. 25
  In Discards .................................... 1
    Invalid BOOTP Information .................... 0
    Invalid DHCP ACK ............................. 0
    Invalid DHCP Release or Decline .............. 0
    Invalid IP/UDP Header ........................ 0
    Max Bindings Exceeded ........................ 1

  Option 82 Insert Error ....................... 0

  Option 82 Received Invalid ................... 0

  Option 82 Received On Untrusted Port ......... 0

  Option 82 Transmit On Untrusted Port ......... 0
    Reply Received On Untrusted Port ............. 0
    Source MAC/CHADDR Mismatch ................... 0
    Static Entry Already Exists .................. 0
Interface ....................................... port1.0.5, All counters 0
Interface ....................................... port1.0.6, All counters 0
```

Table 60: Parameters in the output from the **show ip dhcp snooping statistics** command

Parameter	Description
`Interface`	The interface name.
`In Packets`	The total number of incoming packets that are processed by DHCP Snooping.
`In BOOTP Requests`	The total number of incoming BOOTP Requests.
`In BOOTP Replies`	The total number of incoming BOOTP Replies.
`In Discards`	The total number of incoming packets that have been discarded.
`Invalid BOOTP Information`	Packet contained invalid BOOTP information, such as an invalid BOOTP.OPCode.
`Invalid DHCP ACK`	A DHCP ACK message was discarded, for reasons such as missing Server Option or Lease Option.

Table 60: Parameters in the output from the **show ip dhcp snooping statistics** command (cont.)

Parameter	Description
`Invalid DHCP Release or Decline`	A DHCP Release or Decline message was discarded, for reasons such as mismatch between received interface and current binding information.
`Invalid IP/UDP Header`	A problem was detected in the IP or UDP header of the packet.
`Max Bindings Exceeded`	Accepting the packet would cause the maximum number of bindings on a port to be exceeded.
`Option 82 Insert Error`	An error occurred while trying to insert DHCP Relay Agent Option 82 information.
`Option 82 Received Invalid`	The DHCP Relay Agent Option 82 information received did not match the information inserted by DHCP Snooping.
`Option 82 Received On Untrusted Port`	A packet containing DHCP Relay Agent Option 82 information was received on an untrusted port.
`Option 82 Transmit On Untrusted Port`	A packet containing DHCP Relay Agent Option 82 information was to be sent on an untrusted port.
`Reply Received On Untrusted Port`	A BOOTP reply was received on an untrusted port.
`Source MAC/CHADDR Mismatch`	The L2 Source MAC address of the packet did not match the client hardware address field (BOOTP.CHADDR).
`Static Entry Already Exists`	An entry could not be added as a static entry already exists.

Related commands

clear ip dhcp snooping statistics

ip dhcp snooping

ip dhcp snooping violation

show ip source binding

Overview Use this command to display static entries in the DHCP snooping database. These are the entries that have been added by using the ip source binding command.

Syntax

```
show ip source binding
```

Mode User Exec and Privileged Exec

Example To display static entries in the DHCP snooping database information, use the command:

```
awplus# show ip source binding
```

Table 61: Example output from the **show ip source binding** command

```
awplus# show ip source binding

IP Source Bindings:

Client       MAC                                Expires
IP Address   Address         VLAN  Port         (sec)      Type
-------------------------------------------------------------------
 1.1.1.1     0000.1111.2222  1     port1.0.1    Infinite   Static
```

Table 62: Parameters in the output from the **show ip source binding** command

Parameter	Description
`Client IP Address`	The IP address of the DHCP client.
`MAC Address`	The MAC address of the DHCP client.
`VLAN`	The VLAN ID the packet is received on.
`Port`	The Layer 2 port name the packet is received on.
`Expires (sec)`	Always infinite for static bindings, or when the leave time in the DHCP message was 0xffffffff (infinite).
`Type`	DHCP Snooping binding type: Static

Related commands ip source binding

show ip dhcp snooping binding

51 OpenFlow Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure the OpenFlow protocol.

Command List

- "openflow" on page 2502
- "openflow controller" on page 2503
- "openflow datapath-id" on page 2505
- "openflow failmode" on page 2506
- "openflow inactivity" on page 2508
- "openflow native vlan" on page 2509
- "openflow ssl peer certificate" on page 2510
- "openflow ssl trustpoint" on page 2511
- "openflow version" on page 2512
- "show openflow config" on page 2513
- "show openflow coverage" on page 2515
- "show openflow flows" on page 2517
- "show openflow rules" on page 2520
- "show openflow ssl" on page 2522
- "show openflow status" on page 2523

openflow

Overview Use this command to specify a port or static aggregator as a data plane port. The ingress and egress traffic on the data plane port become controlled by the OpenFlow Controller. A data plane port number is assigned to the port automatically.

Use the **no** variant of this command to cancel the setting of a port as a data plane port.

Syntax

```
openflow
no openflow
```

Default All the ports are non-data plane ports by default.

Mode Interface mode for a switch port (e.g. port1.0.1) or static aggregator (e.g. sa1)

Example To specify port1.0.1 as a data plane port:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# openflow
```

Related commands show openflow config

Command changes Version 5.4.6-1.1: command added

Version 5.4.7-1.1: command added to GS900MX, XS900MX, x550 series products

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

openflow controller

Overview Use this command to specify the controller name, address, and port number of the OpenFlow Controller. If you do not specify a controller name, a name will automatically be created using the following format: 'ocxx', where 'xx' is the sequential number starting from 1.

You can specify one or more OpenFlow Controllers to the switch.

Use the **no** variant of this command to delete one or more OpenFlow Controllers specified to the switch.

You can delete a controller by specifying only the controller name. If you do not know the controller name, you can identify it from the **show openflow config** command output.

Syntax

```
openflow controller <protocol> <address> <port>
openflow controller <controller-name> <protocol> <address>
<port>
no openflow controller <controller-name>
```

Parameter	Description
<controller-name>	The user specified or auto-generated (in the case of legacy syntax) controller name that can contain alphanumeric and/or special characters other than the following set of characters: ':', '=', '', '[', ']', '{', '}', '!', '<', '>'
<protocol>	The protocol type to communicate with the OpenFlow Controller. There are two options: TCP and SSL. Use TCP for an insecure connection. Use SSL for a connection protected by TLS. OpenFlow switches support TLSv1.0, TLSv1.1 and TLSv1.2. The TLS version used between an OpenFlow switch and OpenFlow Controller is determined by peer negotiation.
<address>	The IPv4 address of the Controller.
<port>	Port number used to communicate with the Controller. The IANA has assigned the number 6653 for this purpose, but a different number can be used for local reasons.

Default No OpenFlow Controller is configured by default.

Mode Global Configuration

Usage notes The older version of this command is supported. If you enter the legacy CLI syntax (without the controller name), it will automatically adapt and display in the running configuration as the newer syntax.

For example, entering the legacy command:

```
awplus(config)# openflow controller tcp 192.168.1.2 6653
```

Displays as following in the running-config:

```
awplus(config)# openflow controller oc1 tcp 192.168.1.2 6653
```

Examples To add an OpenFlow Controller with the address 10.1.1.1 using the TCP protocol and the IANA assigned port number of 6653, use the commands:

```
awplus# configure terminal
awplus(config)# openflow controller tcp 10.1.1.1 6653
```

To add an OpenFlow Controller for the switch whose name is controller1, with the address 10.1.2.1 using the TCP protocol on port number 6653, use the commands:

```
awplus# configure terminal
awplus(config)# openflow controller controller1 tcp 10.1.2.1
6653
```

To delete an OpenFlow Controller whose name is controller1, use the commands:

```
awplus# configure terminal
awplus(config)# no openflow controller controller1
```

Related commands show openflow config

Command changes Version 5.4.7-1.1: command added

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

Version 5.4.8-2.1: <*controller-name*> parameter added

openflow datapath-id

Overview Use this command to change the Datapath Identifier (DPID) of the OpenFlow switch.

Use the **no** variant of this command to revert back to the default DPID.

Syntax

```
openflow datapath-id <dpid>
no openflow datapath-id
```

Parameter	Description
<dpid>	The DPID field consists of 16 Hex digits. If you specify a DPID less than 16 Hex digits, then the upper bits are padded out with zeros.

Default Each OpenFlow instance on a switch is identified by a Datapath Identifier. This is a 64 bit number. By default, the lower 48 bits are configured based on the switch MAC address. The top 16 bits are padded with zeros.

Mode Global Configuration

Usage notes This command changes the DPID, which is used as the OpenFlow switch ID in OpenFlow Controller(s).

Example To change the DPID to "0000000000000001", use the commands:

```
awplus# configure terminal
awplus(config)# openflow datapath-id 1
```

To revert back to the default DPID, use the commands:

```
awplus# configure terminal
awplus(config)# no openflow datapath-id
```

Related commands show openflow status

Command changes Version 5.4.7-1.1: command added

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

openflow failmode

Overview Use this command to set the operation mode for the switch when the Controller connection fails or no Controllers are defined.

Use the **no** variant of this command to return to the default mode.

Syntax

```
openflow failmode secure non-rule-expired
openflow failmode standalone
no openflow failmode
```

Parameter	Description
`secure non-rule-expired`	Set the mode to secure non-rule-expired. See the Usage section for details.
`standalone`	Set the mode to standalone. See the Usage section for details.

Default Secure mode, without the **non-rule-expired** option

Mode Global Configuration

Usage notes If an OpenFlow switch loses contact with all Controllers as a result of echo request timeouts, then the OpenFlow switch goes into **fail mode**. There are three fail modes available:

- In **standalone** mode, if no message is received from the OpenFlow Controller for three times the inactivity probe interval, then OpenFlow will take over responsibility for setting up flows. OpenFlow will cause the switch to act like an ordinary MAC-learning switch, but continue to retry connecting to the Controller in the background. When the connection succeeds, it will discontinue its standalone behavior.

  NOTE: *If the OpenFlow switch is in fail mode, and you change the configured fail mode to or from standalone mode, OpenFlow will flush all existing rules.*

- In **secure** mode, OpenFlow will not set up new flows on its own when the Controller connection fails or when no Controllers are defined, but all existing flows are left in place. The switch will continue to retry connecting to any defined Controllers forever, unless a rule timeout causes it to expire.

  This mode is the default, and you can also set it by using the command **no openflow failmode**.

- In **secure non-rule-expired** mode, OpenFlow will not set up new flows on its own when the Controller connection fails or when no Controllers are defined, but all existing flows are left in place. The switch will continue to retry connecting to any defined Controllers forever. The **non-rule-expired** parameter means that existing rules won't be expired regardless of their timeouts while under fail mode. In other words, the OpenFlow switch will ignore timeout values of both *idle timeout* and *hard timeout* in existing rules.

Example

To set the fail mode to **standalone** mode, use the commands:

```
awplus# configure terminal
awplus(config)# openflow failmode standalone
```

To set the fail mode to **secure non-rule-expired** mode, use the commands:

```
awplus# configure terminal
awplus(config)# openflow failmode secure non-rule-expired mode
```

To revert the fail mode to the default mode, use the commands:

```
awplus# configure terminal
awplus(config)# no openflow failmode
```

Related commands

openflow controller

Command changes

Version 5.4.7-1.1: command added

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.1: non-rule-expired parameter added

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

openflow inactivity

Overview Use this command to set the value of the Controller inactivity timeout.

Use the **no** variant of this command to reset the inactivity timeout value to its default.

Syntax

```
openflow inactivity <5-2073600>
no openflow inactivity
```

Parameter	Description
<5-2073600>	Specifies the timeout value in seconds
inactivity	OpenFlow inactivity probe

Default 10 seconds.

Mode Global Configuration

Usage notes OpenFlow uses the inactivity probe timer to monitor its connection to Controller(s). If no message is received from any Controller for three times the inactivity probe interval, then OpenFlow will take over responsibility for setting up flows, if in standalone mode.

Example To configure the inactivity probe timeout to 20 seconds, enter the commands:

```
awplus# configure terminal
awplus(config)# openflow inactivity 20
```

To reset the inactivity probe timeout to its default value of 10 seconds, enter the commands:

```
awplus# configure terminal
awplus(config)# no openflow inactivity
```

Related commands openflow controller

Command changes Version 5.4.7-1.1: command added

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

openflow native vlan

Overview Use this command to specify a VLAN as a native VLAN for the data plane ports. You must create a VLAN (using the vlan database command) before specifying the VLAN as a native VLAN.

The OpenFlow native VLAN **must** be different from the native VLAN of the control plane. This prevents the OpenFlow ports from receiving any broadcast or multicast traffic flooded on the control plane native VLAN.

The VLAN used as the OpenFlow native VLAN should not be used on non-OpenFlow ports.

Use the **no** variant of this command to change the native VLAN for the data plane ports back to the default VLAN 1.

Syntax

```
openflow native vlan <vlan-id>
no openflow native vlan
```

Parameter	Description
<vlan-id>	VLAN ID in the range <1-4090>

Default The native VLAN for the data plane ports is VLAN 1 by default.

Mode Global Configuration

Example To specify VLAN 100 as a native VLAN for the data plane ports:

```
awplus# configure terminal
awplus(config)# openflow native vlan 100
```

To change the native VLAN for the data plane ports back to the VLAN 1:

```
awplus# configure terminal
awplus(config)# no openflow native vlan
```

Related commands show openflow config

Command changes Version 5.4.6-1.1: command added

Version 5.4.7-1.1: command added to GS900MX, XS900MX, x550 series products

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

openflow ssl peer certificate

Overview Use this command to enable a peer certificate to be sent from the machine that the OpenFlow Controller is running.

Use the **no** variant of this command to disable a peer certificate from being sent from the machine that the OpenFlow Controller is running.

Syntax

```
openflow ssl peer certificate {<file>|bootstrap}
no openflow ssl peer certificate
```

Parameter	Description
<file>	The CA certificate of an OpenFlow Controller must be in PEM format and specified with an absolute path using the format flash:cacert.pem. You must copy the file from the machine on which the OpenFlow Controller is running beforehand to the OpenFlow switch.
bootstrap	In bootstrap mode, when the switch first connects to the OpenFlow Controller, it accepts and saves to RAM a self-signed CA certificate sent from the Controller. Thereafter, the OpenFlow switch will only connect to OpenFlow Controllers signed by the same CA certificate.

Default Peer certificate validation is disabled by default.

Mode Global Configuration

Usage notes This command enables or disables peer certification on an OpenFlow Controller.

Example To validate a peer certificate using the bootstrap mode, use the commands:

```
awplus# configure terminal
awplus(config)# openflow ssl peer certificate bootstrap
```

To disable peer certificate validation, use the commands:

```
awplus# configure terminal
awplus(config)# no openflow ssl peer certificate
```

Related commands show openflow ssl

openflow controller

Command changes Version 5.4.7-1.1: command added

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

openflow ssl trustpoint

Overview Use this command to configure the local trustpoint to be used for authentication.

Use the **no** variant of this command to disable the local trustpoint.

Syntax

```
openflow ssl trustpoint local
no openflow ssl trustpoint local
```

Default There is no trustpoint configured by default.

Mode Global Configuration mode.

Usage notes Use this command to specify a local self-signed certificate authority trustpoint for authentication. You must first create the trustpoint using the **crypto pki trustpoint** command.

Example To configure a local trustpoint, use the commands:

```
awplus# configure terminal
awplus(config)# openflow ssl trustpoint local
```

To delete the local trustpoint, use the command:

```
awplus(config)# no openflow ssl trustpoint
```

Related commands openflow controller

openflow ssl trustpoint

Command changes Version 5.4.7-1.1: command added

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

openflow version

Overview Use this command to change the supported OpenFlow version numbers on the switch. You can specify a list of version numbers.

Use the **no** variant of this command to change the version number of the OpenFlow protocol back to the default version 1.3.

Syntax

```
openflow version <version-list>
no openflow version
```

Parameter	Description
<version-list>	Specifies a list of version numbers separated by a space. The version numbers are 1.0 and 1.3.

Default The OpenFlow version is set to 1.3 by default.

Mode Global Configuration

Usage notes This command overwrites any previously configured OpenFlow versions with the default OpenFlow version 1.3.

Example To change the OpenFlow protocol version to 1.0 and 1.3:

```
awplus(config)# openflow version 1.0 1.3
```

To change the OpenFlow protocol version to the default 1.3:

```
awplus(config)# no openflow version
```

Related commands show openflow config

Command changes Version 5.4.6-1.1: command added

Version 5.4.7-1.1: command added to GS900MX, XS900MX, x550 series products

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

show openflow config

Overview Use this command to display the OpenFlow configuration database on the switch.

Syntax
```
show openflow config
```

Mode User Exec/Privileged Exec

Example To show the contents of the OpenFlow configuration database on the switch:
```
awplus# show openflow config
```

Output Figure 51-1: Example output from **show openflow config**

```
awplus# show openflow config
258a3d74-d349-4d18-9d75-09ab66e19d81
    Bridge of0
        Controller "tcp:192.168.1.2:6653"
            is_connected: true
        fail_mode: standalone
        Port of0
            Interface of0
                type: internal
        Port port1.0.4
           Interface port1.0.4
                type: system
                options: {ifindex="5004", mtu="1500", native_vlan="4090"}
        Port port1.0.8
            Interface port1.0.8
                type: system
                options: {ifindex="5008", mtu="1500", native_vlan="4090"}
...
```

Table 51-1: Parameters in the output from **show openflow config**

Parameter	Description
`First line`	The switch ID
`Bridge of0`	The configuration of the OpenFlow bridge.
`Controller`	The address of the OpenFlow Controller and SSL port number
`is_connected: true`	Indicates that the switch is connected to the OpenFlow Controller. If the switch is not connected to the Controller, "is_connected" is not displayed.

Table 51-1: Parameters in the output from **show openflow config** (cont.)

Parameter	Description
`fail_mode`	The fail mode. When the fail mode is "secure," OpenFlow on the switch does not set up flows when the OpenFlow Controller fails. When the fail mode is "standalone", OpenFlow on the switch sets up flows to work as a Layer 2 switch when the OpenFlow Controller fails.
`Port`	The port information
`Interface`	The interface of the port.
`type:`	The type of the port
`options:`	The options for the port

Related commands

openflow controller

openflow native vlan

show openflow status

Command changes

Version 5.4.6-1.1: command added

Version 5.4.7-1.1: command added to GS900MX, XS900MX, x550 series products

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

show openflow coverage

Overview Use this command to display the OpenFlow counters from the Open vSwitch.

Syntax

```
show openflow coverage
```

Mode User Exec/Privileged Exec

Usage The information displayed by this command is for troubleshooting. Contact Allied Telesis Technical Support for assistance.

Example To show OpenFlow counters:

```
awplus# show openflow coverage
```

Output Figure 51-2: Example output from **show openflow coverage**

```
awplus# show openflow coverage
Event coverage, avg rate over last: 5 seconds, last minute, last hour,
hash=86bbd699:
netlink_sent               0.0/sec     0.000/sec        0.0000/sec   total: 14
netlink_recv_jumbo         0.0/sec     0.000/sec        0.0000/sec   total: 4
netlink_received           0.0/sec     0.000/sec        0.0000/sec   total: 49
nln_changed                0.0/sec     0.000/sec        0.0000/sec   total: 18
vconn_sent                 0.0/sec     0.000/sec        0.4703/sec   total: 1801
vconn_received             0.0/sec     0.000/sec        0.4594/sec   total: 1768
vconn_open                 0.4/sec     0.267/sec        0.2372/sec   total: 876
util_xalloc              370.2/sec   354.183/sec      416.7711/sec   total: 1590959
unixctl_replied            0.0/sec     0.017/sec        0.0028/sec   total: 10
unixctl_received           0.0/sec     0.017/sec        0.0028/sec   total: 10
stream_open                0.4/sec     0.267/sec        0.2372/sec   total: 877
pstream_open               0.0/sec     0.000/sec        0.0000/sec   total: 6
rconn_sent                 0.0/sec     0.000/sec        0.4219/sec   total: 1606
rconn_queued               0.0/sec     0.000/sec        0.4219/sec   total: 1606
poll_zero_timeout          0.0/sec     0.033/sec        0.0875/sec   total: 362
poll_create_node          60.6/sec    55.967/sec       68.2844/sec   total: 256721
txn_success                0.2/sec     0.200/sec        0.1953/sec   total: 734
txn_incomplete             0.2/sec     0.267/sec        0.2622/sec   total: 994
txn_unchanged              0.0/sec     0.000/sec        0.0019/sec   total: 34
netdev_get_stats           1.2/sec     1.200/sec        1.1850/sec   total: 4411
netdev_sent                0.0/sec     0.000/sec        0.1219/sec   total: 475
netdev_received            0.0/sec     0.000/sec        0.2608/sec   total: 1005
hmap_expand               10.0/sec     9.433/sec       11.0714/sec   total: 42476
hmap_pathological          0.0/sec     0.000/sec        0.0000/sec   total: 58
hindex_expand              0.0/sec     0.000/sec        0.0006/sec   total: 3
miniflow_malloc            0.0/sec     0.000/sec        0.2611/sec   total: 1008
flow_extract               0.0/sec     0.000/sec        0.0006/sec   total: 5
```

```
dpif_flow_del              0.0/sec     0.000/sec        0.1342/sec   total: 516
dpif_flow_put              0.0/sec     0.000/sec        0.0014/sec   total: 5
dpif_flow_flush            0.0/sec     0.000/sec        0.0000/sec   total: 2
dpif_port_add              0.0/sec     0.000/sec        0.0000/sec   total: 25
cmap_shrink                0.0/sec     0.000/sec        0.2939/sec   total: 1157
cmap_expand                0.0/sec     0.000/sec        0.0006/sec   total: 3
ttp_rev_flow_table         0.0/sec     0.000/sec        0.1050/sec   total: 410
ttp_rev_port_toggled       0.0/sec     0.000/sec        0.0000/sec   total: 2
ttp_rev_reconfigure        0.0/sec     0.000/sec        0.0006/sec   total: 20
xlate_actions              0.0/sec     0.000/sec        0.3969/sec   total: 1530
revalidate_missed_dp_flow  0.0/sec     0.000/sec        0.1356/sec   total: 521
handler_duplicate_upcall   0.0/sec     0.000/sec        0.1258/sec   total: 483
ofproto_update_port        0.0/sec     0.000/sec        0.0000/sec   total: 29
ofproto_recv_openflow      0.0/sec     0.000/sec        0.4111/sec   total: 1573
ofproto_queue_req          0.0/sec     0.000/sec        0.0003/sec   total: 1
ofproto_packet_out         0.0/sec     0.000/sec        0.0006/sec   total: 4
ofproto_flush              0.0/sec     0.000/sec        0.0000/sec   total: 1
bridge_reconfigure         0.0/sec     0.000/sec        0.0000/sec   total: 19
72 events never hit
```

Table 51-2: Parameters in the output from

Parameter	Description
`Event coverage`	The name of a coverage event
`avg rate over last: 5 seconds`	The rate at which the event occurred for the last 5 seconds
`last minute`	The rate at which the event occurred for the last one minute
`last hour`	The rate at which the event occurred for the last one hour
`hash`	The name of the internal hash on the counter
`total:`	The total number of occurrences of the event
`events never hit`	The number of coverage events that have never occurred. When the value is 0, this information is not displayed.

Related commands

show openflow status

show openflow flows

Command changes

Version 5.4.6-1.1: command added

Version 5.4.7-1.1: command added to GS900MX, XS900MX, x550 series products

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

show openflow flows

Overview Use this command to display all the entries in the switch's flow tables that resulted from receiving packets on OpenFlow ports.

Syntax

```
show openflow flows
```

Mode Privileged Exec

Usage notes The switch uses OpenFlow rules from the Controller to create a rule table that tells the switch what to do with packets. From the rules, the switch creates a software flow table to process packets. From the software flow table, the switch creates entries in its silicon hardware flow tables, when possible. When silicon table entries exist, the switch uses them to switch packets. When silicon table entries do not exist, the switch uses the software flow table to process packets.

See the "Communication and Packet Processing" section of the OpenFlow Feature Overview and Configuration Guide for a detailed explanation of how the switch puts entries into the software and silicon flow tables.

This command displays flows in both the software and silicon flow tables. A symbol at the start of each flow output indicates whether it is a silicon or software table entry:

- # indicates silicon flow table entries, and
- ~ indicates software flow table entries

Example To show the entries of the flow tables on the switch:

```
awplus# show openflow flows
```

Output Where possible, the switch uses OpenFlow rules from the Controller to create entries in its silicon hardware flow tables, and switches packets according to the silicon flow tables.

In the following example output, the OpenFlow ports are port1.0.14, port1.0.15, port1.0.16, port1.0.33 and sa3 (port1.0.27 and port1.0.38). As LOCAL and LAG ports are now supported, the first OpenFlow port number is used as the local port.

OpenFlow port numbering becomes:

- port1.0.14 is OpenFlow port number 2
- port1.0.15 is OpenFlow port number 3
- port1.0.33 is OpenFlow port number 5
- sa3 is OpenFlow port number 6

The clients are connected to port1.0.15 and port1.0.33 in this scenario and sa3 is used as OpenFlow ports for the uplink. The **show openflow flows** command shows the following:

Figure 51-3: Example output from **show openflow flows**

```
awplus# show openflow flows

~recirc_id(0),in_port(3),eth(src=08:00:27:9a:b6:7f,dst=08:00:27:4b:ef:3b),eth_type(0
x0800),ipv4(frag=no), packets:0, bytes:0, used:never,
actions:push_vlan(vid=79,pcp=0),6

~recirc_id(0),in_port(6),eth(dst=08:00:27:96:2d:48),eth_type(0x8100),vlan(vid=79,pcp
=0),encap(eth_type(0x0806)), packets:1, bytes:64, used:8.990s, actions:pop_vlan,5

~recirc_id(0),in_port(6),eth(dst=08:00:27:9a:b6:7f),eth_type(0x8100),vlan(vid=79,pcp
=0),encap(eth_type(0x0800),ipv4(frag=no)), packets:1, bytes:346, used:3.938s,
actions:pop_vlan,3

#recirc_id(0),in_port(6),eth(dst=ff:ff:ff:ff:ff:ff/01:00:00:00:00:00),eth_type(0x080
0),ipv4(frag=no), packets:28, bytes:2019, used:2.110s, actions:drop

~recirc_id(0),in_port(5),eth(src=08:00:27:96:2d:48,dst=08:00:27:4b:ef:3b),eth_type(0
x0806), packets:0, bytes:0, used:never, actions:push_vlan(vid=79,pcp=0),6
```

NOTE: *This output includes added line spacing for readability purposes*

Table 51-3: Parameters in the output from **show openflow flows**

Parameter	Description
`recirc_id`	Used to select the next packet processing steps among multiple instances of recirculation. Packets initially enter the process with an ID of 0, which indicates no recirculation.
`in_port`	The OpenFlow port number
`eth`	The source and destination MAC address of the packet
`eth_type`	The Ethernet type
`ipv4`	The information in the IPv4 header
`packets`	The number of matched packets
`bytes`	The number of matched bytes
`actions`	A set of actions for the packets that match the key

Related commands

show openflow coverage

show openflow rules

Command changes

Version 5.4.6-1.1: command added

Version 5.4.7-1.1: command added to GS900MX, XS900MX, x550 series products

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

show openflow rules

Overview Use this command to display the software flow table and rules set by the OpenFlow controller.

Syntax

```
show openflow rules
```

Mode User Exec/Privileged Exec

Example To show the contents of the flow table on the switch:

```
awplus# show openflow rules
```

Output Figure 51-4: Example output from **show openflow rules**

```
awplus# show openflow rules
duration=14s, n_packets=0, n_bytes=0,
priority=399,in_port=1,dl_src=ec:cd:6d:c4:21:bd,actions=drop

duration=14s, n_packets=0, n_bytes=0,
priority=399,in_port=2,dl_src=ec:cd:6d:c4:21:bd,actions=drop

duration=14s, n_packets=0, n_bytes=0,
priority=399,in_port=3,dl_src=ec:cd:6d:c4:21:bd,actions=drop

duration=14s, n_packets=0, n_bytes=0,
priority=399,in_port=4,dl_src=ec:cd:6d:c4:21:bd,actions=drop

duration=14s, n_packets=0, n_bytes=0,
priority=299,in_port=1,dl_dst=00:00:00:00:00:00/01:00:00:00:00:00,
actions=goto_table:2duration=14s, n_packets=0, n_bytes=0,
priority=298,in_port=1,actions=goto_table:3duration=14s,
n_packets=0, n_bytes=0,
priority=99,arp,actions=CONTROLLER:65535duration=14s, n_packets=0,
n_bytes=0,
priority=99,udp,tp_dst=67,actions=CONTROLLER:65535duration=14s,
n_packets=0, n_bytes=0, priority=0,actions=drop

table_id=1, duration=14s, n_packets=0, n_bytes=0,
priority=99,dl_dst=00:00:00:00:00:00/01:00:00:00:00:00,actions=got
o_table:2table_id=1, duration=14s, n_packets=0, n_bytes=0,
priority=0,actions=droptable_id=2, duration=14s, n_packets=0,
n_bytes=0, priority=98,in_port=1,actions=drop
```

```
table_id=2, duration=14s, n_packets=0, n_bytes=0,
priority=97,actions=output:1table_id=2, duration=14s, n_packets=0,
n_bytes=0, priority=0,actions=drop

table_id=3, duration=14s, n_packets=0, n_bytes=0,
priority=0,actions=drop

table_id=254, duration=85668s, n_packets=0, n_bytes=0,
priority=2,recirc_id=0,actions=drop

table_id=254, duration=85668s, n_packets=736, n_bytes=144050,
priority=0,reg0=0x1,actions=controller(reason=no_match)

table_id=254, duration=85668s, n_packets=19, n_bytes=5668,
priority=0,reg0=0x2,actions=drop
```

Table 51-4: Parameters in the output from **show openflow rules**

Parameter	Description
duration	The duration of the flow entry in seconds
n_packets	The number of packets that match the flow entry
n_bytes	The number of bytes that match the flow entry
priority	The priority of the flow entry
in_port	The OpenFlow port number on which the packets are received
dl_src	The source address
dl_dst	The destination address
actions	A set of actions applied to a packet. The actions are: “drop”, “goto_table”, “pop_vlan”, or “push_vlan”
table_id	The table ID of the flow entry

Related commands

show openflow flows

show openflow coverage

Command changes

Version 5.4.6-1.1: command added

Version 5.4.7-1.1: command added to GS900MX, XS900MX, x550 series products

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

show openflow ssl

Overview Use this command to display the current SSL configuration for OpenFlow.

Syntax

```
show openflow ssl
```

Mode Privileged Exec

Usage notes This command displays the current SSL configuration for OpenFlow.

Example To display the current SSL configuration for OpenFlow, use the command:

```
awplus# show openflow ssl
```

Output Figure 51-5: Example output from **show openflow ssl**

```
awplus#show openflow ssl
Private key: /flash/.certs/pki/local/cakey.pem
Certificate: /flash/.certs/pki/local/cacert.pem
CA Certificate: /etc/openvswitch/cacert.pem
Bootstrap: true
```

Related commands

openflow ssl trustpoint

openflow controller

openflow ssl peer certificate

Command changes

Version 5.4.7-1.1: command added

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

show openflow status

Overview Use this command to display the status of each data plane port and the OpenFlow protocol messages queried by the OpenFlow Controller.

Syntax

```
show openflow status
```

Mode Privileged Exec

Example To show the status of a switch with four OpenFlow ports, enter the command:

```
awplus# show openflow status
```

Output Figure 51-6: Example output from **show openflow status**

```
awplus#show openflow status
 OFPT_FEATURES_REPLY (OF1.3) (xid=0x2): dpid:0000eccd6dc421bd
n_tables:254, n_buffers:0
capabilities: FLOW_STATS TABLE_STATS PORT_STATS GROUP_STATS
QUEUE_STATS
OFPST_PORT_DESC reply (OF1.3) (xid=0x3):
 1(port1.0.1): addr:ec:cd:6d:c4:21:bd
     config:     0
     state:      0
     current:    1GB-FD
     supported:  1GB-FD
     speed: 1000 Mbps now, 1000 Mbps max
 2(port1.0.2): addr:ec:cd:6d:c4:21:bd
     config:     0
     state:      LINK_DOWN
     current:    AUTO_NEG
     supported:  1GB-FD
     speed: 0 Mbps now, 1000 Mbps max
 3(port1.0.3): addr:ec:cd:6d:c4:21:bd
     config:     0
     state:      0
     current:    1GB-FD
     supported:  1GB-FD
     speed: 1000 Mbps now, 1000 Mbps max
 4(port1.0.4): addr:ec:cd:6d:c4:21:bd
     config:     0
     state:      LINK_DOWN
     current:    AUTO_NEG
     supported:  1GB-FD
     speed: 0 Mbps now, 1000 Mbps max
LOCAL(of0): addr:1e:f3:f8:c7:13:df
     config:     0
     state:      0
     current:    10MB-FD
     speed: 10 Mbps now, 0 Mbps max
OFPT_GET_CONFIG_REPLY (OF1.3) (xid=0x5): frags=normal
miss_send_len=0
```

Table 51-5: Parameters in the output from **show openflow status**

Parameter	Description
`OFPT_FEATURES_REPLY (OF1.3) (xid=0x2):`	Indicates that the following information is from the OpenFlow version 1.3 Feature reply.
`dpid:`	The datapath ID
`n_tables`	The number of tables supported by the switch
`n_buffers`	The maximum number of packets that the switch can buffer when sending packets to the OpenFlow controller
`capabilities`	A list of the OpenFlow capabilities: FLOW_STATS (flow statistics), TABLE_STATS (table statistics), PORT_STATS (port statistics), IP_REASM (IP fragments reassemble), QUEUE_STATS (queue statistics), and GROUP_STATS (group statistics
`OFPST_PORT_DESC replay (OF1.3) (xid=0x3):`	Indicates that the following information is from the OpenFlow version 1.3 Port Description Reply.
`1(port1.0.1): addr:ec:cd:6d:c4: 21:bd`	The port number and MAC address.
`config:`	The port status: 0 (the port is up) or PORT_DOWN (the port is down.)
`state:`	The link status: 0 (the link is up) or LINK_DOWN (the link is down.)
`current:`	The current feature status.
`supported:`	A list of the supported features: 1GB-FD, 10GB-FD, AUTO-NEG, etc. Not displayed from software release 5.4.7 onwards for interfaces that do not have this capability, i.e. static LAG interfaces or the of0 bridge interface.
`speed:`	The current port speed and maximum speed.
`OFPT_GET_CONFIG_REPLY (OF1.3) (xid=0x5):`	Indicates that the switch responds to a configuration request by an OFPT_GET_CONFIG_REPLY message with the following information.

Table 51-5: Parameters in the output from **show openflow status** (cont.)

Parameter	Description
`frags:`	The action for the IP fragments: normal, dropped, or reassembled. Normal means that an attempt should be made to pass the fragments through the OpenFlow tables.
`miss_send_len=0:`	The number of bytes of each packet that was sent to the OpenFlow controller when a flow table fails or reaches the controller

Related commands

show openflow flows

show openflow rules

show openflow config

Command changes

Version 5.4.6-1.1: command added

Version 5.4.7-1.1: command added to GS900MX, XS900MX, x550 series products

Version 5.4.7-2.1: command added to IE300, IE500 series products

Version 5.4.8-0.2: added to SBx908 GEN2

Version 5.4.8-1.1: added to IE210L series products

Part 6: Network Availability

52 VRRP Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure the Virtual Router Redundancy Protocol (VRRP). For more information, see the VRRP Feature Overview and Configuration Guide.

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

Command List

- "advertisement-interval" on page 2529
- "alternate-checksum-mode" on page 2531
- "circuit-failover" on page 2532
- "debug vrrp" on page 2534
- "debug vrrp events" on page 2535
- "debug vrrp packet" on page 2536
- "disable (VRRP)" on page 2537
- "enable (VRRP)" on page 2538
- "preempt-mode" on page 2539
- "priority" on page 2541
- "router ipv6 vrrp (interface)" on page 2543
- "router vrrp (interface)" on page 2545
- "show debugging vrrp" on page 2547
- "show running-config router ipv6 vrrp" on page 2548
- "show running-config router vrrp" on page 2549
- "show vrrp" on page 2550
- "show vrrp counters" on page 2552
- "show vrrp ipv6" on page 2555

- "show vrrp (session)" on page 2556
- "transition-mode" on page 2558
- "undebug vrrp" on page 2560
- "undebug vrrp events" on page 2561
- "undebug vrrp packet" on page 2562
- "virtual-ip" on page 2563
- "virtual-ipv6" on page 2565
- "vrrp vmac" on page 2567

advertisement-interval

Overview Use this command to configure the advertisement interval of the virtual router. This is the length of time, in seconds, between each advertisement sent from the master to its backup(s).

IPv6 VRRP advertisements are sent to the multicast address assigned to the VRRP group (ff02:0:0:0:0) and a backup virtual router has to join all multicast groups within this range. VRRP advertisements are sent to a multicast address (ff02::12) every second by default.

Use the **no** variant of this command to remove an advertisement interval of the virtual router, which has been set using the **advertisement-interval** command, and revert to the default advertisement interval of 1 second.

Syntax

```
advertisement-interval [<1-255>|csec <1-4095>]
no advertisement-interval
```

Parameter	Description
<1-255>	Specifies the advertisement interval in seconds.
csec	Use centiseconds instead of seconds for the advertisement interval.
<1-4095>	Specifies the advertisement interval in centiseconds.

Default The default advertisement interval is 1 second.

Mode Router Configuration

Usage notes See the VRRP Feature Overview and Configuration Guide for more information about:

- setting the advertisement-interval when configuring VRRP
- using seconds for VRRPv2 host compatibility whenever you use transition-mode to upgrade or transition from VRRPv2 to VRRPv3
- VRRPv3 IPv4 configuration details
- VRRPv3 IPv6 configuration details

Examples The example below shows you how to configure the advertisement interval to 6 seconds for the VRRP IPv4 session with VR ID 5 on interface vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# advertisement-interval 6
```

The example below shows you how to reset the advertisement interval to the default of 1 second for the VRRP IPv4 session with VR ID 5 on interface vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# no advertisement-interval
```

The example below shows you how to configure the advertisement interval to 6 seconds for the VRRPv3 IPv6 session with VR ID 5 on interface vlan2:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 5 vlan2
awplus(config-router)# advertisement-interval 6
```

Related commands

router vrrp (interface)

router ipv6 vrrp (interface)

alternate-checksum-mode

Overview Use this command to enable an alternate checksum mode for VRRPv3 to allow inter-operability with some other vendors' products. The IPv4 checksum for VRRPv3 advertisements will then use a pseudo header in the calculation.

This mode may be required if the other product indicates checksum errors on VRRP packets sent by AlliedWare Plus devices.

Use the **no** variant of this command to disable the alternate checksum mode.

Syntax

```
alternate-checksum-mode
no alternate-checksum-mode
```

Default Disabled

Mode Router Configuration

Example To turn on the alternate checksum mode for VRRP instance 1 on VLAN1, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 1 vlan1
awplus(config-router)# alternate-checksum-mode
```

To turn off the alternate checksum mode for VRRP instance 1 on VLAN1, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 1 vlan1
awplus(config-router)# no alternate-checksum-mode
```

Related commands show running-config

Command changes Version 5.4.7-1.1: command added

circuit-failover

Overview Use this command to enable the VRRP circuit failover feature.

Circuit failover enables the device to take action if the uplink interface goes down, so that the VRRP backup, whose uplink interface is still active, takes over as VRRP master. See the Usage section below and the VRRP Feature Overview and Configuration Guide for more information.

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

Syntax

```
circuit-failover <interface> <1-253>
no circuit-failover [<interface> <1-253>]
```

Parameter	Description
<interface>	The interface of the router that is monitored. The interface must exist on the router, and is usually an upstream interface. Should the interface go down, then another router that is configured as a backup router in the group takes over as the master. You should configure the circuit failover on an interface other than the active VRRP interface - generally the uplink interface.
<1-253>	Delta value. The value by which virtual routers decrement their priority value during a circuit failover event. Configure this value to be greater than the difference of priorities on the master and backup routers. In the case of failover, this priority delta value is subtracted from the current VR Master Router priority value.

Mode Router Configuration

Usage notes You can use Circuit Failover to monitor up to 32 interfaces per VRRP instance. If a VRRP instance is configured to monitor multiple interfaces, the VRRP priority will be cumulatively decremented by the configured delta for each interface as it goes down.

For example, if VRRP is configured to monitor VLAN2 and VLAN3 with the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip address 192.168.1.1/24
awplus(config-if)# exit
awplus(config)# router vrrp 1 vlan1
awplus(config-router)# virtual-ip 192.168.1.10 backup
awplus(config-router)# priority 100
awplus(config-router)# circuit-failover vlan2 10
awplus(config-router)# circuit-failover vlan3 20
```

then the following examples explain the effect of each VLAN going down:

- If only VLAN2 fails, then the VRRP priority will be decremented by 10. VRRP priority would be adjusted to become 90, because 100 - 10 = 90.
- If only VLAN3 fails, then the VRRP priority will be decremented by 20. VRRP priority would be adjusted to become 80, because 100 - 20 = 80.
- If both VLAN2 and VLAN3 fail, then the VRRP priority will be decremented by the cumulative delta values of all monitored interfaces. VRRP priority would therefore be adjusted to become 70, because 100 - 10 - 20 = 70.

As each monitored interface recovers, the VRRP priority is incremented by the same delta value.

When you configure the delta values of the monitored interfaces, make sure their sum is high enough to ensure that the VRRP priority stays above zero if all the interfaces go down.

Examples To configure circuit failover on an IPv4 VRRP instance, so that if interface VLAN3 goes down, then the priority of VRRP instance 1 is reduced by 30, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 1 vlan2
awplus(config-router)# circuit-failover vlan3 30
```

To remove all configured circuit failovers for the VRRP IPv4 session with VR ID 1 on interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 1 vlan2
awplus(config-router)# no circuit-failover
```

To configure circuit failover on a VRRPv3 IPv6 session with VR ID 1, so that when interface VLAN3 goes down, the priority of VRRP instance 1is reduced by 30, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 1 vlan2
awplus(config-router)# circuit-failover vlan3 30
```

To remove all configured circuit failovers for the VRRPv3 IPv6 session with VR ID 1 on interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 1 vlan2
awplus(config-router)# no circuit-failover
```

Related commands router vrrp (interface)

router ipv6 vrrp (interface)

debug vrrp

Overview Use this command to specify debugging options for VRRP. The **all** parameter turns on all the debugging options.

Use the **no** variant of this command to disable this function.

Syntax

```
debug vrrp [all]
no debug vrrp [all]
```

Mode Privileged Exec and Global Configuration

Usage notes See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 debugging details.

Examples The example below shows you how to enable all debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp all
```

The example below shows you how to disable all debugging for VRRP:

```
awplus# configure terminal
awplus(config)# no debug vrrp all
```

Related commands show debugging vrrp

undebug vrrp

debug vrrp events

Overview Use this command to specify debugging options for VRRP event troubleshooting.

Use the **no** variant of this command to disable this function.

Syntax

```
debug vrrp events
no debug vrrp events
```

Mode Privileged Exec and Global Configuration

Usage notes The **debug vrrp events** command enables the display of debug information related to VRRP internal events.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 debugging details.

Examples The example below shows you how to enable events debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp events
```

The example below shows you how to disable events debugging for VRRP:

```
awplus# configure terminal
awplus(config)# no debug vrrp events
```

Related commands show debugging vrrp

undebug vrrp events

debug vrrp packet

Overview Use this command to specify debugging options for VRRP packets.

Use the **no** variant of this command to disable this function.

Syntax

```
debug vrrp packet [send|recv]
no debug vrrp packet [send|recv]
```

Parameter	Description
`send`	Specifies the debug option set for sent packets.
`recv`	Specifies the debug option set for received packets.

Mode Privileged Exec and Global Configuration

Usage notes The **debug vrrp packet** command enables the display of debug information related to the sending and receiving of packets.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 debugging details.

Examples The example below shows you how to enable received and sent packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp packet
```

The example below shows you how to enable only received packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp packet recv
```

The example below shows you how to enable only sent packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp packet send
```

The example below shows you how to disable packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# no debug vrrp packet
```

Related commands show debugging vrrp

undebug vrrp packet

disable (VRRP)

Overview Use this command to disable a VRRP IPv4 session or a VRRPv3 IPv6 session on the router to stop it participating in virtual routing. Note that when this command is configured then a backup router assumes the role of master router depending on its priority. See the enable (VRRP) command to enable a VRRP IPv4 session or a VRRPv3 IPv6 session on the router.

Syntax

```
disable
```

Mode Router Configuration

Usage notes See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 and IPv6 configuration details.

Examples The example below shows you how to disable the VRRP session for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# disable
```

The example below shows you how to disable the VRRPv3 session for VRRPv3 VR ID 3 on vlan1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# disable
```

Related commands

enable (VRRP)

router vrrp (interface)

router ipv6 vrrp (interface)

show vrrp

enable (VRRP)

Overview Use this command to enable the VRRP session on the router to make it participate in virtual routing. To make changes to the VRRP configuration, first disable the router from participating in virtual routing using the disable (VRRP) command.

Syntax

```
enable
```

Mode Router Configuration

Usage notes You must configure the virtual IP address and define the interface for the VRRP session (using the virtual-ip or virtual-ipv6 and the router vrrp (interface) or router ipv6 vrrp (interface) commands) before using this command.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 and IPv6 configuration details.

Examples To enable the VRRP session for VRRP VR ID 5 on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# enable
```

To enable the VRRPv3 session for VRRPv3 VR ID 3 on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# enable
```

Related commands

disable (VRRP)

router vrrp (interface)

router ipv6 vrrp (interface)

show vrrp

virtual-ip

virtual-ipv6

preempt-mode

Overview Use this command to configure preempt mode. If preempt-mode is set to **true**, then the highest priority backup will always be the master when the default master is unavailable.

If preempt-mode is set to **false**, then a higher priority backup will not preempt a lower priority backup who is acting as master.

If preempt-mode is set to **true**, an extra parameter is available called **delay-time**. If the delay-time parameter is used, a VRRP router with a higher priority will wait the configured length of time before it preempts the lower priority VRRP router to take over as master.

Syntax

```
preempt-mode {true|false}[delay-time <0-3600>]
```

Parameter	Description
`true`	Preemption is enabled.
`false`	Preemption is disabled.
`delay-time`	Enable preempting but delay the preempt by the amount of seconds specified by the delay-time value. Note, a delay-time of 0 means delayed preempting is disabled.

Default The default is **true**.

Mode Router Configuration

Usage notes When the master router fails, the backup routers come online in priority order—highest to lowest. Preempt mode means that a higher priority back up router will take over the master role from a lower priority back up. Preempt mode set to **true** allows a higher priority backup router to relieve a lower priority backup router.

By default, a preemptive scheme is enabled whereby a higher priority backup virtual router that becomes available takes over from the backup virtual router that was previously elected to become the master virtual router.

This preemptive scheme can be disabled using the **preempt-mode false** command. If preemption is disabled on a backup virtual router that is starting up, and this router has a higher priority than the current master, the higher priority backup will not preempt the current master, and the lower priority master will stay in the master role.

See the VRRP Feature Overview and Configuration Guide for more information about:

- VRRPv3 IPv4 configuration details
- VRRPv3 IPv6 configuration details
- preempt mode and preempt delay-time

Examples

The example below shows you how to configure preempt-mode as true for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# preempt-mode true
```

The example below shows you how to configure preempt-mode as false for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# preempt-mode false
```

The example below shows you how to configure preempt-mode as true for VRRPv3 VR ID 3 on vlan1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# preempt-mode true
```

The example below shows you how to configure preempt-mode as false for VRRPv3 VR ID 3 on vlan1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# preempt-mode false
```

The example below shows you how to configure delay-time as 20 seconds for VRRPv3 VR ID 5 on vlan5:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 5 vlan5
awplus(config-router)# preempt-mode true delay-time 20
```

Related commands

circuit-failover

priority

router vrrp (interface)

router ipv6 vrrp (interface)

priority

Overview Use this command to configure the VRRP router priority within the virtual router. The highest priority router is Master (unless preempt-mode is false).

Use the **no** variant of this command to remove the VRRP router priority within the virtual router, which has been set using the **priority** command.

Syntax

```
priority <1-255>
no priority
```

Parameter	Description
<1-255>	The priority. For the master router, use 255 for this parameter; otherwise use any number from the range <1-254>.

Default Defaults for priority are: **master router**= 255; **backup**= 100.

Mode Router Configuration

Usage notes Priority determines the role that each VRRP router plays and what happens if the master virtual router fails. If a VRRP router owns the IP address of the virtual router and the IP address of the interface, then this VRRP router functions as the master virtual router.

Priority also determines whether a VRRP router functions as a backup virtual router and the order of ascendancy to becoming a master virtual router if the master virtual router fails. Configure the priority of each backup virtual router with a a value of 1 through 254.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 and IPv6 configuration details.

Examples The example below shows you how to configure 101 as the priority for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# priority 101
```

The example below shows you how to remove the priority configured for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# no priority
```

The example below shows you how to configure 101 as the priority for VRRPv3 VR ID 3 on vlan1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# priority 101
```

The example below shows you how to remove the configured priority for VRRPv3 VR ID 3 on vlan1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# no priority
```

Related commands

circuit-failover

preempt-mode

router ipv6 vrrp (interface)

Overview Use this command to configure VRRPv3 for IPv6 and define the interface that will participate in virtual routing to send and receive advertisement messages. This command allows you to enter the Router Configuration mode.

Use the **no** variant of this command to remove the VRRPv3 for IPv6 configuration. Disable the VRRP session before using the **no** variant of this command.

Syntax

```
router ipv6 vrrp <vrid> <interface>
no router ipv6 vrrp <vrid> <interface>
```

Parameter	Description
<vrid>	*<1-255>* The ID of the virtual router VRRPv3 IPv6 session to create.
<interface>	Specify the name of the interface that will participate in the virtual routing. The interface must exist on the router. The interface specified sends and receives VRRPv3 IPv6 advertisement messages.

Mode Global Configuration

Usage notes Use the required *<interface>* placeholder to define the interface that will participate in virtual routing. This interface is used for two purposes - to send/receive advertisement messages and to forward on behalf of the virtual router when in master state.

NOTE: *Configuring a high number of instances may adversely affect the device's performance, depending on the device CPU, the other protocols it is running, and whether you set the advertisement interval to less than 1 second.*

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv6 configuration details.

Examples The example below shows you how to enable a VRRPv3 session with VR ID 3 on vlan2:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan2
awplus(config-router)# enable
awplus(config-router)#
```

The example below shows you how to disable a VRRPv3 session with VR ID 3 on vlan2:

```
awplus(config-router)# disable
awplus(config-router)# exit
awplus(config)# no router ipv6 vrrp 3 vlan2
awplus(config)#
```

Related commands

advertisement-interval

circuit-failover

router vrrp (interface)

Overview Use this command to configure VRRP IPv4 and define the interface that will participate in virtual routing to send and receive advertisement messages. This command allows you to enter the Router Configuration mode.

Use the **no** variant of this command to remove the VRRP IPv4 configuration. Disable the VRRP session before using the **no** variant of this command.

Syntax

```
router vrrp <vrid> <interface>
no router vrrp <vrid> <interface>
```

Parameter	Description
<vrid>	*<1-255>* The ID of the virtual router VRRP IPv4 session to create.
<interface>	Specify the name of the interface that will participate in the virtual routing. The interface must exist on the router. The interface specified sends and receives VRRP IPv4 advertisement messages.

Mode Global Configuration

Usage notes Use the required *<interface>* placeholder to define the interface that will participate in virtual routing. This interface is used for two purposes - to send/receive advertisement messages and to forward on behalf of the virtual router when in master state.

NOTE: *Configuring a high number of instances may adversely affect the device's performance, depending on the device CPU, the other protocols it is running, and whether you set the advertisement interval to less than 1 second.*

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

Examples To enable a VRRP session with VR ID 5 on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan1
awplus(config-router)# enable
```

To disable a VRRP session with VR ID 5 on vlan1, use the commands:

```
awplus(config-router)# disable
awplus(config-router)# exit
awplus(config)# no router vrrp 5 vlan1
```

Related commands

advertisement-interval

circuit-failover

disable (VRRP)

enable (VRRP)

show debugging vrrp

Overview Use this command to display the set VRRP debugging option. Use the terminal monitor command to display output on the console otherwise debug output is in the log file.

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

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 debugging details.

Syntax

```
show debugging vrrp
```

Mode User Exec and Privileged Exec

Example The example below shows you how to display VRRP debugging:

```
awplus# show debugging vrrp
```

Related commands

debug vrrp

debug vrrp events

debug vrrp packet

show running-config router ipv6 vrrp

Overview Use this command to show the running configuration for VRRPv3 IPv6.

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

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv6 configuration details.

Syntax

```
show running-config router vrrp
```

Mode Privileged Exec, Global Configuration, Line Configuration, and Interface Configuration.

Example The example below shows you how to display the running configuration for VRRPv3 IPv6:

```
awplus# show running-config router ipv6 vrrp
```

Output Figure 52-1: Example output from the **show running-config router ipv6 vrrp** command

```
!
router ipv6 vrrp 3 vlan3
 virtual-ip fe80::202:b3ff:fed5:983e master
 circuit-failover vlan3 3
 advertisement-interval 6
 preempt-mode false
!
```

show running-config router vrrp

Overview Use this command to show the running configuration for VRRP IPv4.

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

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

Syntax

```
show running-config router vrrp
```

Mode Privileged Exec, Global Configuration, Line Configuration, and Interface Configuration.

Example The example below shows you how to display the running configuration for VRRP IPv4:

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

Output Figure 52-2: Example output from the **show running-config router vrrp** command

```
!
router vrrp 2 vlan2
 circuit-failover vlan2 2
 advertisement-interval 4
 preempt-mode true
!
```

show vrrp

Overview Use this command to display information about all VRRP IPv4 sessions. This command shows a summary when the optional **brief** parameter is used.

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

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

Syntax

```
show vrrp [brief]
```

Parameter	Description
brief	Brief summary of VRRP sessions.

Mode User Exec and Privileged Exec

Example To display information about all VRRP IPv4 sessions, enter the command:

```
awplus# show vrrp
```

To display brief summary output about VRRP IPv4 sessions, enter the command:

```
awplus# show vrrp brief
```

Output Figure 52-3: Example output from the **show vrrp** command

```
awplus#show vrrp
VMAC enabled
Address family IPv4
VRRP Id: 1 on interface: vlan2
 State: AdminUp    - Master
 Virtual IP address: 192.168.1.2 (Not-owner)
 Priority is 100
 Advertisement interval: 100 centiseconds
 Preempt mode: TRUE
 Multicast membership on IPv4 interface vlan2: JOINED
 Transition mode: FALSE
 Accept mode: FALSE
 Master address: 192.168.1.3
```

Figure 52-4: Example output from the **show vrrp brief** command

```
awplus#show vrrp brief
Interface        Grp  Prio Own  Pre  State      Master addr      Group addr
 vlan10            1   200   N    P  Master     192.168.10.4     192.168.10.253
 vlan10            2   150   N    P  Backup     192.168.10.4     192.168.10.254
 vlan11            3   200   N    P  Master     192.168.11.4     192.168.11.253
 vlan11            4   150   N    P  Backup     192.168.11.4     192.168.11.254
```

Related commands

enable (VRRP)

disable (VRRP)

show vrrp counters

Overview This command displays VRRP SNMP counters on the console, as described in the VRRP MIB and RFC2787, for debugging use while you configure VRRP with commands in this chapter.

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

Syntax

```
show vrrp counters
```

Mode User Exec and Privileged Exec

Usage notes The output has a section for global counters and a section of counters for each VRRP instance configured. See the descriptions of the counters below the sample output as per RFC2787.

NOTE: *Note that the counters displayed with this commands are the same counters as described in RFC 2787 (Copyright (C) The Internet Society (2000). All Rights Reserved) except for the "Monitored Circuit Up" and "Monitored Circuit Down" counters, which are additions beyond the MIB.*

Example To display information about VRRP SNMP counters on the console, enter the command:

```
awplus# show vrrp counters
```

Figure 52-5: Example output from the **show vrrp counters** command

```
awplus#show vrrp counters
VRRP Global Counters:
  Checksum Errors .... 230
  Version Errors ..... 0
  VRID Errors ........ 230

VRRP IPv4 counters for VR 10/vlan10:
  Master Transitions ........ 0
  Received Advertisements ... 0
  Internal Errors ........... 0
  TTL Errors ................ 0
  Received Priority 0 Pkt ... 0
  Sent Priority 0 Pkt ....... 0
  Received Invalid Type ..... 0
  Address List Errors ....... 0
  Packet Length Errors ...... 0
  Monitored Circuit Up ...... 0
  Monitored Circuit Down..... 0
```

```
VRRP IPv4 counters for VR 100/vlan100:
  Master Transitions ........ 1
  Received Advertisements ... 1614
  Internal Errors ........... 0
  TTL Errors ................ 0
  Received Priority 0 Pkt ... 0
  Sent Priority 0 Pkt ....... 0
  Received Invalid Type ..... 0
  Address List Errors ....... 0
  Packet Length Errors ...... 0
  Monitored Circuit Up ...... 0
  Monitored Circuit Down..... 2
```

Table 1: Global counters with descriptions for the **show vrrp counters** command:

Counter	Description
`Checksum Errors`	The total number of VRRP packets received with an invalid VRRP checksum value.
`Version Errors`	The total number of VRRP packets received with an unknown or unsupported version number.
`VRID Errors`	The total number of VRRP packets received with an invalid VRID for this virtual router.

Table 2: Per VR counters with descriptions for the **show vrrp counters** command:

Counter	Description
`Master Transitions`	The total number of times that this virtual router's state has transitioned to MASTER.
`Received Advertisements`	The total number of VRRP advertisements received by this virtual router.
`Internal Errors`	The total number of VRRP advertisement packets received for which the advertisement interval is different than the one configured for the local virtual router.
`TTL Errors`	The total number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
`Received Priority 0 Pkt`	The total number of VRRP packets received by the virtual router with a priority of '`0`'.
`Sent Priority 0 Pkt`	The total number of VRRP packets sent by the virtual router with a priority of '`0`'.
`Received Invalid Type`	The number of VRRP packets received by the virtual router with an invalid value in the '`type`' field.
`Address List Errors`	The total number of packets received for which the address list does not match the locally configured list for the virtual router.

Table 2: Per VR counters with descriptions for the **show vrrp counters** command: (cont.)

Counter	Description
`Packet Length Errors`	The total number of packets received with a packet length less than the length of the VRRP header.
`Monitored Circuit Up`	The total number of times the monitored circuit has generated the UP event.
`Monitored Circuit Down`	The total number of times the monitored circuit has generated the down event.

show vrrp ipv6

Overview Use this command to display information about all configured VRRPv3 IPv6 sessions for all interfaces, or all VRRPv3 IPv6 sessions for a given interface with the optional parameter.

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

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv6 configuration details.

Syntax

```
show vrrp ipv6 [<interface>]
```

Parameter	Description
<interface>	Specify the name of the interface that will participate in the virtual routing. The interface must exist on the router. The interface specified sends and receives VRRPv3 IPv6 advertisement messages.

Mode User Exec and Privileged Exec

Example To display information about all VRRPv3 IPv6 sessions, enter the command:

```
awplus# show vrrp ipv6
```

Output Figure 52-6: Example output from the **show vrrp ipv6 vlan2** command

```
awplus#show vrrp ipv6 vlan2
VrId <1>
 State is Master
 Virtual IP is fe80::202:b3ff:fed5:983e (Owner)
 Interface is vlan2
 Priority is 255
 Advertisement interval is 4 sec
 Preempt mode is FALSE
```

Related commands

enable (VRRP)

disable (VRRP)

show vrrp (session)

Overview Use this command to display information for a particular VRRP session.

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

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

Syntax

```
show vrrp <vrid> <interface>
```

Parameter	Description
<vrid>	*<1-255>* The virtual router ID for which to display information. Session must already exist.
<interface>	The interface to display information about, for instance, `vlan2`.

Mode User Exec and Privileged Exec

Usage notes See the below sample output from the **show vrrp** command displaying information about VRRP session 1 configured on **vlan2**. Output shows that a Virtual IP address has been set.

```
awplus# show vrrp 1 vlan2
```

```
awplus#show vrrp 1 vlan2
Address family IPv4
VrId <1>
 Interface is vlan2
 State is Initialize
 Virtual IP address is 10.10.11.250 (Not IP owner)
 Priority is 100
 Advertisement interval is 1 sec
```

See the below sample output from the **show vrrp** command displaying information about VRRP session 1 configured on **vlan3**. Output shows a Virtual IP address has not been set.

```
awplus# show vrrp 1 vlan3
```

```
awplus#show vrrp 1 vlan3
Address family IPv4
VrId <1>
 Interface is vlan3
 State is Initialize
 Virtual IP address is unset
 Priority is 100
 Advertisement interval is 1 sec
 Preempt mode is TRUE
```

Example The following command shows information about VRRP session 5 for interface **vlan2**.

```
awplus# show vrrp 5 vlan2
```

transition-mode

Overview Use this command to configure the IPv4 transition mode. Transition mode allows you to upgrade from VRRPv2 to VRRPv3 and gives interoperability between VRRPv2 and VRRPv3.

If transition-mode is set to **true**, then the IPv4 transition mode is enabled and VRRPv2 and VRRPv3 advertisements are sent allowing VRRPv2 and VRRPv3 interoperability. Received VRRPv2 advertisement packets are accepted and processed when transition-mode is true.

If transition-mode is set to **false**, then the IPv4 transition mode is disabled and only VRRPv3 advertisements are sent. Received VRRPv2 advertisement packets are dropped.

Note the advertisement-interval should not be configured to less than 1 second when using transition-mode. VRRPv2 can only use advertisements in whole second intervals.

Syntax

```
transition-mode {true|false}
```

Parameter	Description
`true`	Transition mode is enabled. This results in VRRPv2 and VRRPv3 IPv4 advertisements being sent. Transition mode is only available on VRRPv3 for interoperability with VRRPv2 while upgrading to VRRPv3.
`false`	Transition mode is disabled. This stops VRRPv2 IPv4 advertisements being sent. Only VRRPv3 advertisements are sent when disabled. Disable transition-mode after upgrading from VRRPv2 to VRRPv3.

Default The default is **false**.

Mode Router Configuration

Usage notes See the VRRP Feature Overview and Configuration Guide for more information:

- VRRPv3 IPv4 configuration details
- VRRPv3 IPv6 configuration details
- further information about configuring transition mode to upgrade from VRRPv2 to VRRPv3

Examples The example below shows you how to configure IPv4 transition-mode as true for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# transition-mode true
```

The example below shows you how to configure IPv4 transition-mode as false for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# transition-mode false
```

Related commands router vrrp (interface)

undebug vrrp

Overview Use this command to disable all VRRP debugging.

Syntax

```
undebug vrrp all
```

Mode Privileged Exec

Example The example below shows you how to disable all VRRP debugging:

```
awplus# undebug vrrp all
```

Related commands debug vrrp

undebug vrrp events

Overview Use this command to disable debugging options for VRRP event troubleshooting.

Syntax

```
undebug vrrp events
```

Mode Privileged Exec

Example The example below shows you how to disable VRRP event debugging:

```
awplus# undebug vrrp events
```

Related commands debug vrrp events

undebug vrrp packet

Overview Use this command to disable debugging options for VRRP packets.

Syntax

```
undebug vrrp packet [send|recv]
```

Parameter	Description
`send`	Disable the debug option set for sent packets.
`recv`	Disable the debug option set for received packets.

Mode Privileged Exec

Examples The example below shows you how to disable VRRP sent packet debugging:

```
awplus# undebug vrrp packet send
```

The example below shows you how to disable VRRP received packet debugging:

```
awplus# undebug vrrp packet recv
```

The example below shows you how to disable all VRRP packet debugging:

```
awplus# undebug vrrp packet
```

Related commands debug vrrp packet

virtual-ip

Overview Use this command to set the virtual IP address for the VRRP session. This is the IP address of the virtual router that end hosts set as their default gateway.

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

Syntax

```
virtual-ip <ip-address> [master|backup|owner]
no virtual-ip
```

Parameter	Description
<ip-address>	The virtual IPv4 address of the virtual router, entered in dotted decimal format A.B.C.D.
`master`	Sets the default state of the VRRP router within the Virtual Router as **master**. For master, the router must own the Virtual IP address. Specify the **owner** option before using **master** option.
`backup`	Sets the default state of the VRRP router within the Virtual Router as **backup**.
`owner`	Sets the IPv6 address of the VRRP router within the Virtual Router as the **owner**. Specify this before using the **master** option.

Mode Router Configuration

Usage notes The VRRP master and owner of the virtual IPv4 address for the VRRP session only responds to the packets destined to the virtual IPv6 address. The VRRP master that is not an owner of the virtual IPv4 address for the VRRP session does not respond to the packets destined to the virtual IPv4 address, but forwards packets with a VMAC as the destination address. See the vrrp vmac command to enable and disable this feature.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

Examples The example below shows you how to set the virtual IP address for VRRP VR ID 5 and the router as the VRRP master:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# virtual-ip 192.0.2.30 master
```

The example below shows you how to set the virtual IPv4 address for VRRP VR ID 5 and the router as the VRRP backup:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# virtual-ip 192.0.2.30 backup
```

The example below shows you how to set the virtual IPv4 address for VRRP VR ID 5 and the router as owner of the virtual IPv4 address:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# virtual-ip 192.0.2.30 owner
```

The example below shows you how to disable the virtual IPv4 address for VRRP VR ID 5

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# no virtual-ip
```

Related commands

router vrrp (interface)

enable (VRRP)

vrrp vmac

virtual-ipv6

Overview Use this command to set the virtual IPv6 address for the VRRPv3 session. This is the IPv6 address of the virtual router that end hosts set as their default gateway.

Note that the primary IPv6 address specified is an IPv6 link-local address. See the Usage note below for further information.

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

Syntax

```
virtual-ipv6 <ipv6-address> [master|backup]
[primary|secondary]
```

```
no virtual-ipv6
```

Parameter	Description
<ipv6-address>	The IPv6 address of the virtual router, entered in hexadecimal, in the format X:X::X.X.
`master`	Sets **master** to be the default state of the VRRPv3 router within the Virtual Router. For **master**, we recommend using a Virtual IP address that is not owned by any of the VRRP routers in the same grouping (that share the same VRID).
`backup`	Sets **backup** to be the default state of the VRRPv3 router within the Virtual Router.
`primary`	Sets the specified address as the primary IPv6 address. The primary address must be a link-local IPv6 address.
`secondary`	Sets the specified address as the secondary IPv6 address. Normally this would be a globally-routable IPv6 address. This enables you to specify a globally-routable address as the default gateway address for all the hosts on a VLAN.

Mode Router Configuration

Usage notes The virtual router will reply to ping, telnet, and SSH requests to the virtual IP address. The virtual router will reply even if it does not own the virtual IP address.

The AlliedWare Plus VRRPv3 implementation supports one IPv6 virtual link local address per virtual router ID. Note that in the command examples fe80::1 is an IPv6 link-local address. An IPv6 link-local address is used because IPv6 link-local addresses are used by IPv6 ND (Neighbor Discovery). A host's default route to a router points to the IPv6 link- local address, not a specific global IPv6 address for the router. For the host's traffic to switch over to a backup router, the IPv6 link-local address of the router is used by VRRPv3.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv6 configuration details.

Examples

The example below shows you how to set the virtual IPv6 address for VRRPv3 VR ID 3 and the router as the VRRPv3 master:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# virtual-ipv6 fe80::1 master
```

The example below shows you how to set the virtual IPv6 address for VRRPv3 VR ID 3 and the router as the VRRPv3 backup:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# virtual-ipv6 fe80::1 backup
```

The example below shows you disable the virtual IPv6 address for VRRPv3 VR ID 3:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# no virtual-ipv6
```

Related commands

router ipv6 vrrp (interface)

enable (VRRP)

vrrp vmac

vrrp vmac

Overview Use this command to enable or disable the VRRP Virtual MAC feature. This feature is used by VRRP to make the hosts use the virtual MAC address as the physical hardware address of their gateway.

A VRRP router master will use the virtual MAC address for any ARP responses associated with the virtual IP address, or any gratuitous ARPs sent on behalf of the virtual IP address.

All VRRP advertisements are sent using this virtual MAC address as the source MAC address.

The virtual MAC address has the form 00:00:5e:00:01:<VRID>, where VRID is the ID of the Virtual Router.

Syntax

```
vrrp vmac {enable|disable}
```

Mode Global Configuration

Examples To enable Virtual MAC enter:

```
awplus# configure terminal
awplus(config)# vrrp vmac enable
```

To disable Virtual MAC enter:

```
awplus# configure terminal
awplus(config)# vrrp vmac disable
```

Related commands virtual-ip

virtual-ipv6

53 Ethernet Protection Switched Ring (EPSRing™) Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure Ethernet Protection Switched Ring (EPSRing™). For more information, see the EPSR 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

- "debug epsr" on page 2570
- "epsr" on page 2571
- "epsr configuration" on page 2572
- "epsr datavlan" on page 2573
- "epsr enhancedrecovery enable" on page 2574
- "epsr flush-type" on page 2575
- "epsr mode master controlvlan primary port" on page 2577
- "epsr mode transit controlvlan" on page 2578
- "epsr priority" on page 2579
- "epsr state" on page 2580
- "epsr topology-change" on page 2581
- "epsr trap" on page 2582
- "show debugging epsr" on page 2583
- "show epsr" on page 2584
- "show epsr common segments" on page 2589
- "show epsr config-check" on page 2590
- "show epsr <epsr-instance>" on page 2591
- "show epsr <epsr-instance> counters" on page 2592

- "show epsr counters" on page 2593
- "show epsr summary" on page 2594
- "undebug epsr" on page 2595

debug epsr

Overview This command enables EPSR debugging.

The **no** variant of this command disables EPSR debugging.

Syntax

```
debug epsr {info|msg|pkt|state|timer|all}
no debug epsr {info|msg|pkt|state|timer|all}
```

Parameter	Description
`info`	Send general EPSR information to the console. Using this parameter with the **no debug epsr** command will explicitly exclude the above information from being sent to the console.
`msg`	Send the decoded received and transmitted EPSR packets to the console. Using this parameter with the **no debug epsr** command will explicitly exclude the above packets from being sent to the console.
`pkt`	Send the received and transmitted EPSR packets as raw ASCII text to the console. Using this parameter with the **no debug epsr** command will explicitly exclude the above packets from being sent to the console.
`state`	Send EPSR state transitions to the console. Using this parameter with the **no debug epsr** command will explicitly exclude state transitions from being sent to the console.
`timer`	Send EPSR timer information to the console. Using this parameter with the **no debug epsr** command will explicitly exclude timer information from being sent to the console.
`all`	Send all EPSR debugging information to the console. Using this parameter with the **no debug epsr** command will explicitly exclude any debugging information from being sent to the console.

Mode Privileged Exec and Global Configuration

Examples To enable state transition debugging, use the command:

```
awplus# debug epsr state
```

To disable EPSR packet debugging, use the command:

```
awplus# no debug epsr pkt
```

Related commands undebug epsr

epsr

Overview This command sets the timer values for an EPSR instance. These are only valid for master nodes.

NOTE: *Running your switch as an EPSR master node requires a feature license.*

Syntax

```
epsr <epsr-instance> {hellotime <1-32767>|failovertime
<2-65535> ringflaptime <0-65535>}
```

```
no epsr <epsr-instance>
```

CAUTION: *Using the no variant of this command will remove the specified EPSR instance.*

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`hellotime <1-32767>`	The number of seconds between the transmission of health check messages.
`failovertime <2-65535>`	The number of seconds that a master waits for a returning health check message before entering the failed state. **The failover time should be greater than twice the hellotime.** This is to force the master node to wait until it detects the absence of two sequential healthcheck messages before entering the failed state.
`ringflaptime <0-65535>`	The minimum number of seconds that a master must remain in the failed state.

Mode EPSR Configuration

Examples To set the hellotimer to 5 seconds for the EPSR instance called blue, use the command:

```
awplus(config-epsr)# epsr blue hellotime 5
```

To delete the EPSR instance called blue, use the command:

```
awplus(config-epsr)# no epsr blue
```

Related commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

epsr configuration

epsr datavlan

epsr state

epsr trap

show epsr

epsr configuration

Overview Use this command to enter EPSR Configuration mode so that EPSR can be configured.

Syntax

```
epsr configuration
```

Mode Global Configuration

Example To change to EPSR mode, use the command:

```
awplus(config)# epsr configuration
```

Related commands

epsr mode master controlvlan primary port

epsr

show epsr

epsr datavlan

Overview This command adds a data VLAN or a range of VLAN identifiers to a specified EPSR instance.

The **no** variant of this command removes a data VLAN or data VLAN range from an EPSR instance.

Syntax

```
epsr <epsr-instance> datavlan {<vlanid>|<vlanid-range>}
no epsr <epsr-instance> datavlan {<vlanid>|<vlanid-range>}
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
datavlan	Adds a data VLAN to be protected by the EPSR instance.
<vlanid>	The VLAN's VID - a number between 1 and 4094 excluding the number selected for the control VLAN.
<vlanid-range>	Specify a range of VLAN identifiers using a hyphen to separate identifiers.

Mode EPSR Configuration

Usage notes We recommend you

- set the EPSR control VLAN to vlan2, using the epsr mode master controlvlan primary port and epsr mode transit controlvlan commands, then
- set the EPSR data VLAN between to be a value between 3 and 4094, using the epsr datavlan command.

Examples To add `vlan3` to the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue datavlan vlan3
```

To add `vlan2` and `vlan3` to the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue datavlan vlan2-vlan3
```

To remove `vlan3` from the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue datavlan vlan3
```

To remove `vlan2` and `vlan3` from the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue datavlan vlan2-vlan3
```

Related commands epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr

epsr enhancedrecovery enable

Overview This command enables EPSR's enhanced recovery mode. Enhanced recovery mode enables a ring to apply additional recovery procedures when a ring with more than one break partially mends. For more information, see the EPSR Feature Overview and Configuration Guide.

The **no** variant of this command disables the enhanced recovery mode.

Syntax

```
epsr <epsr-instance> enhancedrecovery enable
no epsr <epsr-instance> enhancedrecovery enable
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.

Default Default is that enhanced recovery mode disabled.

Mode EPSR Configuration

Example To apply enhanced recovery on the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue enhancedrecovery enable
```

Related commands show epsr

epsr flush-type

Overview Use this command to set how EPSR flushes Layer 2 entries when a topology change occurs. It can be configured to flush all Layer 2 entries on its EPSR interfaces or only flush the Layer 2 entries on its EPSR data VLANs.

Use the **no** variant of this command to revert to the default setting.

Syntax

```
epsr <epsr-name> flush-type {interface|vlan}
no epsr <epsr-name> flush-type
```

Parameter	Description
<epsr-name>	The name of the EPSR instance to set the flush-type for.
`interface`	Flush all Layer 2 entries from the EPSR interface on a topology change.
`vlan`	Flush the Layer 2 entries on the EPSR interface and data VLANs on a topology change.

Default The default flush-type is vlan

Mode EPSR Configuration

Usage notes To flush all entries on the EPSR interface (including non-EPSR data VLANs) the flush-type command must be explicitly configured on the EPSR ring with the **interface** parameter.

Select **interface** as the flush-type to help reduce latency caused during EPSR topology changes. This type of flushing is quicker and less granular than flushing per data vlan, as flushing on a data **vlan** may incur a higher overhead, reducing EPSR responsiveness to ring topology changes.

Interface flushing can be used to optimize EPSR rings with a large number of VLANs. It will however also require relearning on any VLANs that are on an EPSR interface but not part of the EPSR configuration.

Example To configure the behavior of EPSR ring 'red' transit node on topology changes to flush all Layer 2 entries on its EPSR ring interfaces, use the following commands:

```
awplus# configure terminal
awplus(config)# epsr configuration
awplus(config-epsr)# epsr red mode transit controlvlan 10
awplus(config-epsr)# epsr red datavlan 20-29
awplus(config-epsr)# epsr red flush-type interface
awplus(config-epsr)# epsr red state enable
```

Related commands show epsr

Command changes Version 5.4.9-1.1: command added

epsr mode master controlvlan primary port

Overview This command creates a master EPSR instance. Your switch is unable to run this command because it cannot function as an EPSR master node. To include these switches in an EPSR ring you will need to use an alternative Allied Telesis switch, such as an x550 Series switch, as the master node. For more information on this command, refer to the manual of your master EPSR node's switch.

NOTE: *This command will only run on switches that are capable of running as an EPSR master node. However, even if your switch cannot function as an EPSR master node, you still need to configure this command on whatever switch is the master within your EPSR network.*

NOTE: *Running your switch as an EPSR master node requires a feature license.*

Syntax

```
epsr <epsr-instance> mode master controlvlan <2-4094>
primaryport <port>
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
mode	Determines the node is acting as a master.
master	Sets switch to be the master node for the named EPSR ring.
controlvlan	The VLAN that will transmit EPSR control frames.
<2-4094>	VLAN id.
primaryport	Primary port for the EPSR instance.
<port>	The primary port. The port may be a switch port (e.g. port1.0.4) or a static channel group (e.g. sa3). It cannot be a dynamic (LACP) channel group.

NOTE: *The software allows you to configure more than two ports or static channel groups to the control VLAN within a single switch. However, we advise against this because in certain situations it can produce unpredictable results.*

Mode EPSR Configuration

Example To create a master EPSR instance called blue with vlan2 as the control VLAN and port1.0.1 as the primary port, use the command:

```
awplus(config-epsr)# epsr blue mode master controlvlan vlan2
primaryport port1.0.1
```

Related commands epsr mode transit controlvlan

show epsr

epsr mode transit controlvlan

Overview This command creates a transit EPSR instance.

Syntax

```
epsr <epsr-instance> mode transit controlvlan <2-4094>
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
mode	Determines the node is acting as a transit node.
transit	Sets switch to be the transit node for the named EPSR ring.
controlvlan	The VLAN that will transmit EPSR control frames.
<2-4094>	VLAN id.

NOTE: *The software allows you to configure more than two ports or static channel groups to the control VLAN within a single switch. However, we advise against this because in certain situations it can produce unpredictable results.*

If the control VLAN contains more than two ports (or static channels) an algorithm selects the two ports or channels with the lowest number to be the ring ports. However if the switch has only one channel group is defined to the control vlan, EPSR will not operate on the secondary port.

EPSR does not support Dynamic link aggregation (LACP).

Mode EPSR Configuration

Example To create a transit EPSR instance called `blue` with `vlan2` as the control VLAN, use the command:

```
awplus(config-epsr)# epsr blue mode transit controlvlan vlan2
```

Related commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr

epsr priority

Overview This command sets the priority of an EPSR instance on an EPSR node. Priority is used to prevent "superloops" forming under fault conditions with particular ring configurations. Setting a node to have a priority greater than one, also has the effect of turning on **superloop protection**.

The **no** variant of this command returns the priority of the EPSR instance back to its default value of 0, which also disables EPSR Superloop prevention.

Syntax

```
epsr <epsr-instance> priority <0-127>
no <epsr-instance> priority
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`priority`	The priority of the ring instance selected by the epsr-name parameter.
<0-127>	The priority to be applied (0 is the lowest priority and represents no superloop protection).

Default The default priority of an EPSR instance on an EPSR node is 0. The negated form of this command resets the priority of an EPSR instance on an EPSR node to the default value.

Mode EPSR Configuration

Example To set the priority of the EPSR instance called `blue` to the highest priority (127), use the command:

```
awplus(config-epsr)# epsr blue priority 127
```

To reset the priority of the EPSR instance called `blue` to the default (0), use the command:

```
awplus(config-epsr)# no epsr blue priority
```

Related commands epsr configuration

epsr state

Overview This command enables or disables an EPSR instance.

Syntax

```
epsr <epsr-instance> state {enabled|disabled}
```

Parameter	Description
<epsr-instance>	The name of the EPSR instance.
`state`	The operational state of the ring.
`enabled`	EPSR instance is enabled.
`disabled`	EPSR instance is disabled.

Mode EPSR Configuration

Example To enable the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue state enabled
```

Related commands epsr mode master controlvlan primary port

epsr mode transit controlvlan

epsr topology-change

Overview Use this command to allow the given EPSR instance to accept notifications from other topology protocols, namely G.8032, for Topology Change Notifications (TCN).

Use the **no** variant of this command to return the EPSR instance to where it does not accept TCNs from the other specified protocol, and as a result does not send out a “flush FDB” message.

Syntax

```
epsr <epsr-name> topology-change g8032
no epsr <epsr-name> topology-change g8032
```

Parameter	Description
<epsr-name>	The name of the EPSR instance for which the topology-change applies to.
`topology-change`	The topology-change value to be set for the instance.
`g8032`	Specify that G.8032 is the other protocol that the topology-change notifications are allowed to be accepted from in order to send "flush FDB" messages to other EPSR nodes in the ring.

Default The default value is no notifications are accepted and in turn no “flush FDB” messages are sent.

Mode EPSR Configuration

Usage notes The purpose of this command is to allow EPSR to accept notifications from other topology protocols, namely G.8032, about Topology Change Notifications (TCN). Once EPSR accepts the TCN, it will in turn notify the other nodes on the EPSR ring to perform an FDB flush.

Example To configure an EPSR instance named “red” to accept G.8032 TCNs, use the following command:

```
awplus(config-epsr)# epsr red topology-change g8032
```

To configure an EPSR instance named “red” to no longer accept G.8032 TCNs, use the following command:

```
awplus(config-epsr)# no epsr red topology-change g8032
```

Related commands show epsr

show g8032 erp-instance

Command changes Version 5.4.7-1.1: command added

epsr trap

Overview This command enables SNMP traps for an EPSR instance. The traps will be sent when the EPSR instance changes state.

The **no** variant of this command disables SNMP traps for an EPSR instance. The traps will no longer be sent when the EPSR instance changes state.

Syntax

```
epsr <epsr-instance> trap
no epsr <epsr-instance> trap
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`trap`	SNMP trap for the EPSR instance.

Mode EPSR Configuration

Example To enable traps for the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue trap
```

To disable traps for the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue trap
```

Related commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr

show debugging epsr

Overview This command shows the debugging modes enabled for EPSR.

Syntax

```
show debugging epsr
```

Mode User Exec and Privileged Exec

Example To show the enabled debugging modes, use the command:

```
awplus# show debugging epsr
```

Related commands debug epsr

show epsr

Overview This command displays information about all EPSR instances.

Syntax

```
show epsr
```

Mode User Exec and Privileged Exec

Example To show the current settings of all EPSR instances, use the command:

```
awplus# show epsr
```

Output: non-superloop topology The following examples show the output display for a non-superloop topology network.

Table 1: Example output from the **show epsr** command run on a transit node

```
EPSR Information
-------------------------------------------------------------
 Name ........................ test2
 Mode ........................ Transit
 Status ...................... Enabled
 State ....................... Links-Up
 Control Vlan ................ 2
 Data VLAN(s) ................ 10
 Interface Mode .............. Ports Only
 First Port .................. port1.0.1
 First Port Status ........... Down
 First Port Direction ........ Unknown
 Second Port ................. port1.0.2
 Second Port Status .......... Down
 Second Port Direction ....... Unknown
 Trap ........................ Enabled
 Master Node ................. Unknown
 Enhanced Recovery ........... Disabled
-------------------------------------------------------------
```

Table 2: Example output from the **show epsr** command run on a master node

```
EPSR Information
-------------------------------------------------------------
 Name ....................... test4
 Mode ........................ Master
 Status ...................... Enabled
 State ....................... Complete
 Control Vlan ................ 4
 Data VLAN(s) ................ 20
 Interface Mode .............. Ports Only
 Primary Port ................ port1.0.3
 Primary Port Status ......... Forwarding
 Secondary Port .............. port1.0.4
 Secondary Port Status ....... Forwarding
 Hello Time .................. 1 s
 Failover Time ............... 2 s
 Ring Flap Time .............. 0 s
 Trap ........................ Enabled
 Enhanced Recovery ........... Disabled
-------------------------------------------------------------
```

NOTE: *Running your switch as an EPSR master node requires a feature license.*

Output: superloop topology

The following examples show the output display for superloop topology network.

Table 3: Example output from the **show epsr** command run on a Master Node

```
 EPSR Information
-------------------------------------------------------------
 Name ....................... test4
 Mode ........................ Master
 Status ...................... Enabled
 State ....................... Complete
 Control Vlan ................ 4
 Data VLAN(s) ................ 20
 Interface Mode .............. Ports Only
 Primary Port ................ port1.0.3
   Status .................... Forwarding (logically blocking)
   Is On Common Segment ...... No
   Blocking Control .......... Physical
 Secondary Port .............. port1.0.4
   Status .................... Blocked
   Is On Common Segment ...... No
   Blocking Control .......... Physical
 Hello Time .................. 1 s
 Failover Time ............... 2 s
 Ring Flap Time .............. 0 s
 Trap ........................ Enabled
 Enhanced Recovery ........... Disabled
 SLP Priority ................ 12
-------------------------------------------------------------
```

NOTE: *Running your switch as an EPSR master node requires a feature license.*

Table 4: Example output from the **show epsr** command run on a Transit Node

```
 EPSR Information
-------------------------------------------------------------
 Name ......................... test4
 Mode ......................... Transit
 Status ....................... Enabled
 State ........................ Complete
 Control Vlan ................. 4
 Data VLAN(s) ................. 20
 Interface Mode ............... Ports Only
 Primary Port ................. port1.0.3
   Status ..................... Forwarding (logically blocking)
   Is On Common Segment ....... No
   Blocking Control ........... Physical
 Secondary Port ............... port1.0.4
   Status ..................... Blocked
   Is On Common Segment ....... No
   Blocking Control ........... Physical
 Hello Time ................... 1 s
 Failover Time ................ 2 s
 Ring Flap Time ............... 0 s
 Trap ......................... Enabled
 Enhanced Recovery ............ Disabled
 SLP Priority ................. 12
-------------------------------------------------------------
```

Table 5: Parameters displayed in the output of the **show epsr** command

Parameter on Master Node	Parameter on Transit Node	Description
Name	Name	The name of the EPSR instance.
Mode	Mode	The mode in which the EPSR instance is configured - either Master or Transit
Status	Status	Indicates whether the EPSR instance is enabled or disabled
State	State	Indicates state of the EPSR instance's state machine. Master states are: Idle, Complete, and Failed. Transit states are Links-Up, Links-Down, and Pre-Forwarding.
Control Vlan	Control Vlan	Displays the VID of the EPSR instance's control VLAN.
Data VLAN(s)	Data VLAN(s)	The VID(s) of the instance's data VLANs.
Interface Mode	Interface Mode	Whether the EPSR instance's ring ports are both physical ports (Ports Only) or are both static aggregators (Channel Groups Only).
Primary Port	First Port	The EPSR instance's primary ring port.

Table 5: Parameters displayed in the output of the **show epsr** command (cont.)

Parameter on Master Node	Parameter on Transit Node	Description
- Status	- Status	Whether the ring port is forwarding (Forwarding) or blocking (Blocked), or has link down (Down), and if forwarding or blocking, "(logical)" indicates the instance has only logically set the blocking state of the port because it does not have physical control of it.
	- Direction	The ring port on which the last EPSR control packet was received is indicated by "Upstream". The other ring port is then "Downstream"
- Is On Common Segment	- Is On Common Segment	Whether the ring port is on a shared common segment link to another node, and if so, "(highest rank)" indicates it is the highest priority instance on that common segment.
- Blocking Control	- Blocking Control	Whether the instance has "physical" or "logical" control of the ring port's blocking in the instance's data VLANs.
Secondary Port	Second Port	The EPSR instance's secondary port.
- Status	- Status	Whether the ring port is forwarding (Forwarding) or blocking (Blocked), or has link down (Down), and if forwarding or blocking, "(logical)" indicates the instance has only logically set the blocking state of the port, because it does not have physical control of it. Note that on a master configured for SuperLoop Prevention (non-zero priority) its secondary ring port can be physically forwarding, but logically blocking. This situation arises when it is not the highest priority node in the topology (and so does not receive LINKS-DOWN messages upon common segment breaks) and a break on a common segment in its ring is preventing reception of its own health messages.
	- Direction	The ring port on which the last EPSR control packet was received is indicated by "Upstream". The other ring port is then "Downstream"
- Is On Common Segment	- Is On Common Segment	Whether the ring port is on a shared common segment link to another node, and if so, "(highest rank)" indicates it is the highest priority instance on that common segment
- Blocking Control	- Blocking Control	Whether the instance has "physical" or "logical" control of the ring port's blocking in the instance's data VLANs
Hello Time		The EPSR instance's setting for the interval between transmissions of health check messages (in seconds)
Failover Time		The time (in seconds) the EPSR instance waits to receive a health check message before it decides the ring is down
Ring Flap Time		The minimum time the EPSR instance must remain in the failed state
Trap	Trap	Whether the EPSR instance has EPSR SNMP traps enabled

Table 5: Parameters displayed in the output of the **show epsr** command (cont.)

Parameter on Master Node	Parameter on Transit Node	Description
`Enhanced Recovery`	`Enhanced Recovery`	Whether the EPSR instance has enhanced recovery mode enabled
`SLP Priority`	`SLP Priority`	The EPSR instance's priority (for SuperLoop Prevention)

Related commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr counters

show epsr common segments

Overview This command displays information about all the superloop common segment ports on the switch.

Syntax

```
show epsr common segments
```

Example To display information about all the superloop common segment ports on the switch, use the command:

```
awplus# show epsr common segments
```

Table 6: Example output from the **show epsr common segments** command

```
EPSR Common Segments

Common Seg  EPSR                          Port     Phys Ctrl  Ring
Ring Port   Instance         Mode     Prio  Type     of Port?   Port Status
-------------------------------------------------------------------------------
port1.0.4   test_inst_Red    Transit  127   Second     Yes      Fwding
            test_inst_Blue   Transit  126   Second     No       Fwding (logical)
            test_inst_Green  Transit  125   First      No       Fwding (logical)

sa4         testA            Master    15   Primary    Yes      Blocking
            testB            Transit   14   Second     No       Fwding (logical)

sa5         test_55          Transit    8   First      Yes      Down
            test_77          Transit    7   First      No       Down
-------------------------------------------------------------------------------
```

Related commands

show epsr

show epsr summary

show epsr counters

show epsr config-check

Overview This command checks the configuration of a specified EPSR instance, or all EPSR instances.

If an instance is enabled, this command will check for the following errors or warnings:

- The control VLAN has the wrong number of ports.
- There are no data VLANs.
- Some of the data VLANs are not assigned to the ring ports.
- The instance is a master with its secondary port on a common segment.

Syntax

```
show epsr [<instance>] config-check
```

Parameter	Description
<instance>	Name of the EPSR instance to check on.

Mode User Exec and Privileged Exec

Example To check the configuration of all EPSR instances and display the results, use the command:

```
awplus# show epsr config-check
```

Table 53-1: Example output from **show epsr config-check**

```
EPSR             Status   Description
Instance
------------------------------------------------------------------------
red              OK.
white            OK.
blue             Warning  Primary port is not in data VLANs 29-99.
orange           OK.

Don't forget to check that this node's configuration is consistant with all
other nodes in the ring.
------------------------------------------------------------------------
```

Related commands show epsr

show epsr <epsr-instance>

Overview This command displays information about the specified EPSR instance.

Syntax

```
show epsr <epsr-instance>
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.

Mode User Exec and Privileged Exec

Example To show the current settings of the EPSR instance called `blue`, use the command:

```
awplus# show epsr blue
```

Related commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr counters

show epsr <epsr-instance> counters

Overview This command displays counter information about the specified EPSR instance.

Syntax

```
show epsr <epsr-instance> counters
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.

Mode User Exec and Privileged Exec

Example To show the counters of the EPSR instance called `blue`, use the command:

```
awplus# show epsr blue counters
```

Related commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr

show epsr counters

Overview This command displays counter information about all EPSR instances.

Syntax

```
show epsr counters
```

Mode User Exec and Privileged Exec

Example To show the counters of all EPSR instances, use the command:

```
awplus# show epsr counters
```

Related commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr

show epsr summary

Overview This command displays summary information about all EPSR instances on the switch

Syntax
```
show epsr summary
```

Mode User Exec and Privileged Exec

Example To display EPSR summary information, use the command:

```
awplus# show epsr summary
```

Table 54: Example output from the **show epsr summary** command

```
EPSR Summary Information

Abbreviations:
  M = Master node
  T = Transit node
  C = is on a common segment with other instances
  P = instance on a common segment has physical control of the shared port's
        data VLAN blocking
  LB = ring port is Logically Blocking - applicable to master only

EPSR                                  Ctrl       Primary/1st     Secondary/2nd
Instance      Mode Status   State     VLAN  Prio Port Status     Port Status
-------------------------------------------------------------------------------
test-12345      T  Enabled  Links-Down    6  127  Blocking (C,P)  Blocking (C,P)
test1           M  Enabled  Complete      5   12  Fwding          Fwding (LB)
test2           T  Enabled  Pre-Fwding    4  126  Fwding (C)      Blocking (C)
localB          T  Disabled Idle         40    0  Unknown         Unknown
localC          T  Disabled Idle         41    0  Unknown         Unknown
-------------------------------------------------------------------------------
```

undebug epsr

Overview This command applies the functionality of the **no** variant of the debug epsr command.

54 G.8032 Ethernet Ring Protection Switching Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure G.8032 Ethernet Ring Protection Switching.

For more information, see the G.8032 Ethernet Ring Protection Switching Feature Overview and Configuration Guide.

Command List

- "cfm-sf-notify" on page 2598
- "clear g8032 erp-instance" on page 2600
- "clear g8032 erp-instance statistics" on page 2602
- "data-traffic" on page 2603
- "debug g8032" on page 2605
- "enable (g8032-profile)" on page 2606
- "epsr topology-change" on page 2607
- "erp-instance" on page 2608
- "g8032 erp-instance" on page 2609
- "g8032 forced-switch erp-instance" on page 2611
- "g8032 manual-switch erp-instance" on page 2613
- "g8032 physical-ring" on page 2614
- "g8032 profile" on page 2616
- "level (g8032-switch)" on page 2617
- "physical-ring" on page 2618
- "profile name" on page 2619
- "raps-channel" on page 2620
- "service onm" on page 2621

- "rpl role" on page 2622
- "show debugging g8032" on page 2624
- "show g8032 erp-instance" on page 2625
- "show g8032 erp-instance statistics" on page 2630
- "show g8032 physical-ring" on page 2632
- "show g8032 profile" on page 2634
- "sub-ring" on page 2636
- "timer (g8032-profile)" on page 2637
- "topology-change" on page 2639
- "trap (g8032-switch)" on page 2641
- "undebug g8032" on page 2642

cfm-sf-notify

Overview Use this command to configure this ERP instance to receive signal fail notifications from a Local MEP(s). This command can be used multiple times to allow multiple Local MEPs to be specified.

Use the **no** variant of this command to remove a Local MEP from sending notifications to this G.8032 ERP instance.

Syntax

```
cfm-sf-notify mep mpid <mep-id> domain <domain-name> service
<ma-name>
```

```
no cfm-sf-notify mep mpid <mep-id> domain <domain-name> service
<ma-name>
```

Parameter	Description
`mep`	Specify that a Local Maintenance End Point (MEP) is to provide the Signal Fail notification to this G.8032 ERP instance.
`mpid`	Specify that the Local MEP is to be identified by MEP-id.
`<mep-id>`	1-8191. Specify the Local MEP's ID.
`domain`	Specify the Maintenance Domain that the Local MEP is associated with.
`<domain-name>`	Specify the Maintenance Domain's CLI instance name.
`service`	Specify the Maintenance Association that the Local MEP is associated with.
`<ma-name>`	Specify the Maintenance Association's CLI instance name.

Mode G8032 Configure Switch

Usage notes CFM and Continuity Check Messaging (CCM) can be configured to detect link faults on the East or West interface ports as a whole, or faults on the R-APS VLAN on the East or West interface. In this situation CFM Local MEPs can notify G.8032 of defects it detects. G.8032 will treat these notifications as a Signal Fail (SF) for that East or West ring port. Similarly, CFM Local MEPs can notify G.8032 that the fault has cleared. When this command is used, this G.8032 ERP instance will ensure that the specified Local MEP is a Down MEP for the East or West interface used by this instance or for the R-APS VLAN on the East or West interface used by this instance.

Example To configure an ERP instance to receive signal fail notifications from a local MEP with an MEP ID of “12”, an MD named “MD-INST1”, and an MA named “MA-INST1-1”, use the following commands:

```
awplus(config)# g8032 erp-instance ring2
```

```
awplus(g8032-config-switch)# cfm-sf-notify mep mpid 12 domain
MD-INST1 service MA-INST1-1
```

Related commands

ethernet cfm domain-name

ethernet cfm mep

g8032 erp-instance

service ma-name

show g8032 erp-instance

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

clear g8032 erp-instance

Overview Use this command to:

- trigger a reversion immediately, without waiting for timers to expire, or
- clear a forced-switch or manual-switch command that was previously successfully entered on a G.8032 Ethernet Ring Protection (ERP) instance.

Syntax

```
clear g8032 erp-instance <erp-instance-name>
```

Parameter	Description
<erp-instance-name>	The name of the G.8032 ERP instance

Mode Privileged Exec

Usage notes This command can be used after a protection switch has occurred and the failure has cleared. If reversion is enabled, this command will trigger a reversion immediately, without having to wait for certain timers to expire (such as WTB or WTR). If reversion has been disabled, this command will trigger a reversion.

Alternatively, this command can be used on an ERP instance where a forced-switch or manual-switch command has been successfully entered to clear that action. The command will be ignored if a force-switch or manual-switch command had not been previously entered successfully, even if such node is in the FORCED_SWITCH or MANUAL_SWITCH state.

Examples To trigger a reversion immediately without waiting for a timer to expire on an ERP instance named “blue”, use the following command:

```
awplus# clear g8032 erp-instance blue
```

Alternatively, to clear a previously applied forced-switch from an ERP instance named “blue”, use the following command:

```
awplus# clear g8032 erp-instance blue
```

The forced-switch would be created using a command like this one, which forces a protection switch on the East interface of an ERP instance named “blue”:

```
awplus# g8032 forced-switch erp-instance blue east-interface
```

Related commands

g8032 erp-instance

g8032 forced-switch erp-instance

g8032 manual-switch erp-instance

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

clear g8032 erp-instance statistics

Overview Use this command to clear the statistics data being collected by a G.8032 Ethernet Ring Protection (ERP) instance.

Syntax

```
clear g8032 erp-instance <erp-instance-name> statistics
```

Parameter	Description
<erp-instance-name>	The name of a specific G.8032 ERP instance

Mode Privileged Exec

Usage notes A G.8032 ERP instance keeps statistical data as counts on a variety of data such as the number of certain types of Ring-Automatic Protection Switching (R-APS) messages sent and received over its ring port(s) and error conditions detected. Use this command to clear the statistics data.

Example To clear the statistics for an ERP instance named “blue”, use the following command:

```
awplus# clear g8032 erp-instance blue statistics
```

Related commands

g8032 erp-instance

show g8032 erp-instance statistics

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

data-traffic

Overview Use this command to add a data traffic VLAN or a range of VLANs to be protected by this G.8032 Ethernet Ring Protection (ERP) instance.

Use the **no** variant of this command to remove a data traffic VLAN or a range of VLANs.

Syntax

```
data-traffic <vid-list>
no data-traffic <vid-list>
```

Parameter	Description
<vid-list>	The data traffic VLAN ID(s). This can be a single VLAN ID, or can be a range of VLAN IDs separated by hyphen, or a comma separated list of VLAN IDs and ranges. Each VLAN ID can take on the range of 1 to 4094

Mode G8032 Configure Switch

Usage notes

- A G.8032 ERP instance can protect 0, 1 or more VLANs carrying data traffic.
- This ERP instance must be associated with a physical ring instance.
- Other ERP instances using the same physical ring instance are not allowed to have the same data traffic VLAN(s) as this ERP instance.
- The data VLAN(s) must already exist.
- The data VLAN(s)' port members should be members of the ring interface(s), but it is not enforced.
- When a data traffic VLAN(s) is removed, any blocks that were in place on the ring ports for this VLAN(s) are removed. The user should make sure when removing the VLAN(s) from the ERP instance that a loop is not formed.
- Data traffic VLAN(s) can be added or removed while the ERP instance is enabled or disabled.

Example To add a data traffic VLAN with a VLAN ID of "103" to an ERP instance named "blue", use the following commands:

```
awplus(config)# g8032 erp-instance blue
awplus(g8032-config-switch)# data-traffic 103
```

Related commands g8032 erp-instance

show g8032 erp-instance

Command changes Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

debug g8032

Overview Use this command to enable G.8032 debugging.

Use the **no** variant of this command to disable G.8032 debugging.

Syntax

```
debug g8032 {all|event|rx|tx}
no debug g8032 {all|event|rx|tx}
```

Parameter	Description
`all`	Turn on all G.8032 debugging
`event`	Turn on G.8032 Event debugging
`rx`	Turn on G.8032 Receive debugging
`tx`	Turn on G.8032 Transmit debugging

Mode Privileged Exec

Example To enable all G.8032 debugging, use the following command:

```
awplus# debug g8032 all
```

Related commands

show debugging

show debugging g8032

undebug g8032

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

enable (g8032-profile)

Overview Use this command to change the revertive or non-revertive operation of the associated G.8032 Ethernet Ring Protection (ERP) instance.

Syntax

```
enable {revertive|non-revertive}
```

Parameter	Description
`revertive`	This allows the ERP instance associated with this profile to operate in revertive mode.
`non-revertive`	This allows the ERP instance associated with this profile to operate in non- revertive mode.

Default By default, the mode of operation is revertive.

Mode G8032 Profile Configuration

Usage notes An ERP instance uses a profile which contains timer configurations and configurations for revertive modes of operation. Once a ring failure has abated, a G.8032 ring instance will check its mode of operation, and if the mode is revertive, it will attempt to revert back to where the RPL-Owner controls the blocking of the ring. Otherwise, it operates in non-revertive mode.

Example To enable revertive mode for a profile named “prof_1”, use the following commands:

```
awplus(config)# g8032 profile prof_1
awplus(g8032-profile-config)# enable revertive
```

Related commands

g8032 profile

show g8032 profile

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

epsr topology-change

Overview Use this command to allow the given EPSR instance to accept notifications from other topology protocols, namely G.8032, for Topology Change Notifications (TCN).

Use the **no** variant of this command to return the EPSR instance to where it does not accept TCNs from the other specified protocol, and as a result does not send out a “flush FDB” message.

Syntax

```
epsr <epsr-name> topology-change g8032
no epsr <epsr-name> topology-change g8032
```

Parameter	Description
<epsr-name>	The name of the EPSR instance for which the topology-change applies to.
`topology-change`	The topology-change value to be set for the instance.
`g8032`	Specify that G.8032 is the other protocol that the topology-change notifications are allowed to be accepted from in order to send "flush FDB" messages to other EPSR nodes in the ring.

Default The default value is no notifications are accepted and in turn no “flush FDB” messages are sent.

Mode EPSR Configuration

Usage notes The purpose of this command is to allow EPSR to accept notifications from other topology protocols, namely G.8032, about Topology Change Notifications (TCN). Once EPSR accepts the TCN, it will in turn notify the other nodes on the EPSR ring to perform an FDB flush.

Example To configure an EPSR instance named “red” to accept G.8032 TCNs, use the following command:

```
awplus(config-epsr)# epsr red topology-change g8032
```

To configure an EPSR instance named “red” to no longer accept G.8032 TCNs, use the following command:

```
awplus(config-epsr)# no epsr red topology-change g8032
```

Related commands show epsr

show g8032 erp-instance

Command changes Version 5.4.7-1.1: command added

erp-instance

Overview Use this command to enable or disable a G.8032 Ethernet Ring Protection (ERP) instance.

Syntax

```
erp-instance {enabled|disabled}
```

Parameter	Description
`enabled`	The G.8032 ERP instance is enabled
`disabled`	The G.8032 ERP instance is disabled

Default The ERP instance is disabled.

Mode G8032 Configure Switch

Usage notes Once a G.8032 ERP instance has been configured with the correct parameter settings or defaults, it can be enabled to run the G.8032 protocol. To change certain ERP instance parameters, the instance may need to be disabled.

When enabled, the instance is restarted back to the G8032_ST_INIT state. In this state, if the node has an RPL-Owner or RPL-Neighbor port, it will be blocked. Otherwise the node will block one of its ring ports. All the nodes will send Ring-Automatic Protection Switching (R-APS) messages initially. The G.8032 protocol and state machines will transition the ring into another more appropriate state.

When disabled, the ERP instance will no longer process incoming R-APS messages for that instance, nor send any R-APS messages. The raps-channel VLAN and any data-traffic VLANs used by this instance will be put in the forwarding state for its physical ring ports. Caution should be taken to avoid loops when disabling an ERP instance.

Example To enable an ERP instance named “blue”, use the following commands:

```
awplus(config)# g8032 erp-instance blue
awplus(g8032-config-switch)# erp-instance enabled
```

Related commands

g8032 erp-instance

show g8032 erp-instance

trap (g8032-switch)

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

g8032 erp-instance

Overview Use this command to create a G.8032 Ethernet Ring Protection (ERP) instance, or to enter an existing instance's context.

Use the **no** variant of this command to destroy the specified instance.

Syntax

```
g8032 erp-instance <erp-instance-name>
no g8032 erp-instance <erp-instance-name>
```

Parameter	Description
<erp-instance-name>	The name of the G.8032 ERP instance. This can be up to 32 characters.

Mode Global Configuration

Usage notes The ERP protocol in AlliedWare Plus™ can run one or more instances. A G.8032 ERP instance is made up of:

- two ERP ring ports,
- a Control VLAN that carries Ring-Automatic Protection Switching (R-APS) messages, and
- zero, one, or more Protected traffic data VLANs that the instance protects when the ring fails.

An ERP instance must be associated with a G.8032 physical ring and a G.8032 profile.

Example To enter the context of an instance named “blue”, use the following commands:

```
awplus(config)# g8032 erp-instance blue
awplus(g8032-config-switch)#
```

Related commands

clear g8032 erp-instance

clear g8032 erp-instance statistics

data-traffic

erp-instance

g8032 forced-switch erp-instance

g8032 manual-switch erp-instance

level (g8032-switch)

physical-ring

profile name

raps-channel

rpl role

show g8032 erp-instance

show g8032 erp-instance statistics

sub-ring

topology-change

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

g8032 forced-switch erp-instance

Overview Use this command to force a protection switch on a G.8032 Ethernet Ring Protection (ERP) instance ring port.

Syntax
```
g8032 forced-switch erp-instance <erp-instance-name>
{east-interface|west-interface|terminating-interface}
```

Parameter	Description
<erp-instance-name>	The name of the G.8032 ERP instance
east-interface	The G.8032 ERP instance's East ring port
west-interface	The G.8032 ERP instance's West ring port
terminating-interface	The G.8032 ERP instance's Terminating ring port

Mode Privileged Exec

Usage notes G.8032 supports a Forced Protection Switch action initiated by the operator. A Forced Protection Switch command is to be issued at a given G.8032 node and given port in the ring. This results in a block being applied at that ring port (and an unblock on the opposite ring port), and a R-APS designated Forced Switch message to flow around the ring causing the RPL to become unblocked.

Multiple Forced Switch actions can take place along a G.8032 ring. Care must be taken when using the Force Switch command as it can only be undone by issuing a Clear command and not by a failure nor the clearing of a failure. If a node that was issued a Force Switch command later fails, then it becomes difficult to remove the Force Switch condition from the ring. In this situation, the operator has to go to the nodes that are adjacent to the failed node, and for each one, issue a Forced Switch command on the ring link facing the failed node followed by a Clear command.

If the G.8032 Physical Ring instance associated with the specified ERP instance is set to terminating-interface, then only one ring port is available and terminating-interface must be used in this command, otherwise specify the east-interface or the west-interface.

To clear this action command, use the clear g8032 erp-instance command.

Example To issue a Forced Protection Switch on the East interface of an ERP instance named “blue”, use the following command:

```
awplus# g8032 forced-switch erp-instance blue east-interface
```

Related commands clear g8032 erp-instance

g8032 erp-instance

Command changes Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

g8032 manual-switch erp-instance

Overview Use this command to manually cause a protection switch on a G.8032 Ethernet Ring Protection (ERP) instance ring port.

Syntax
```
g8032 manual-switch erp-instance <erp-instance-name>
{east-interface|west-interface|terminating-interface}
```

Parameter	Description
<erp-instance-name>	The name of the G.8032 ERP instance
east-interface	The G.8032 ERP instance's East ring port
west-interface	The G.8032 ERP instance's West ring port
terminating-interface	The G.8032 ERP instance's Terminating ring port

Mode Privileged Exec

Usage notes G.8032 supports a Manual Protection Switch action initiated by the operator. A Manual Protection Switch command is to be issued at a given G.8032 node and given port in the ring. This results in a block being applied at that ring port (and an unblock on the opposite ring port), and a R-APS designated Manual Switch message to flow around the ring causing the RPL to become unblocked.

The difference between a Manual switch and a Forced switch is that the Manual Switch will be ignored under various conditions. In particular, only one Manual Switch is allowed on a G.8032 ring at a time.

If the G.8032 Physical Ring instance associated with the specified ERP instance is set to terminating-interface, then only one ring port is available and terminating-interface must be used in this command, otherwise specify the east-interface or the west-interface.

To clear this action command, use the clear g8032 erp-instance command.

Example To issue a Manual Protection Switch on the East interface of an ERP instance named “blue”, use the following command:

```
awplus# g8032 manual-switch erp-instance blue east-interface
```

Related commands clear g8032 erp-instance

g8032 erp-instance

Command changes Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

g8032 physical-ring

Overview Use this command to create a G.8032 Ethernet Ring Protection (ERP) physical ring profile which specifies the Ethernet ports that will be used as G.8032 ring ports.

Syntax

```
g8032 physical-ring <physical-ring-name> {east-interface
<interface-name1> west-interface <interface-name2>|
terminating-interface <interface-name>}
```

```
no g8032 physical-ring <physical-ring-name>
```

Parameter	Description
<physical-ring-name>	The name of the profile (up to 37 characters)
east-interface	The East G.8032 ring port
<interface-name1>	The name of the switch interface, either port or channel group, for the East ring port. It must differ from the West ring port.
west-interface	The West G.8032 ring port
<interface-name2>	The name of the switch interface, either port or channel group, for the West ring port. It must differ from the East ring port.
terminating-interface	The Terminating ring port. This should only be used for G.8032 ERP instance that is at the end of a sub-ring.
<interface-name>	The name of the switch interface, either port or channel group, for the Terminating ring port.

Mode Global Configuration

Usage notes Each ERP instance will be associated with a physical ring profile. A physical ring profile is made up of two physical Ethernet ports or aggregated interfaces, unless it is the terminating point of a sub-ring in which case only one port is needed. When two ports are used, they are referred to as East and West ports. When only a single port is used, it is referred to as a Terminating port.

Example To create a physical ring profile named “red” where the East interface port is port1.0.4 and the West interface port is port1.0.8, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# g8032 physical-ring red east-interface
port1.0.4 west-interface port1.0.8
```

Related commands

physical-ring

rpl role

show g8032 physical-ring

sub-ring

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

g8032 profile

Overview Use this command to create a G.8032 Ethernet Ring Protection (ERP) instance profile, or to enter that instance's profile context.

Use the **no** variant of this command to destroy the specified instance.

Syntax

```
g8032 profile {<erp-profile-name>|default-profile}
no g8032 profile <erp-profile-name>
```

Parameter	Description
<erp-profile-name>	The name of the G.8032 profile. This can be up to 32 characters.
default-profile	The name of the system's default profile for G.8032. This profile is created by the system automatically and can not be destroyed.

Default A profile with the name "default-profile" will exist in the system and is used by default by an ERP instance. All the parameters in the default profile take on the default values.

Mode Global Configuration

Example To enter the context of a profile named “prof_1”, use the following commands:

```
awplus(config)# g8032 profile prof_1
awplus(g8032-profile-config)#
```

Related commands

enable (g8032-profile)

profile name

show g8032 profile

timer (g8032-profile)

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

level (g8032-switch)

Overview Use this command to configure the level for Ring-Automatic Protection Switching (R-APS) messages.

Syntax

```
level <0-7>
```

Parameter	Description
<0-7>	The level used by the G.8032 ERP instance.

Default The default level is 0.

Mode G8032 Configure Switch

Usage notes Inside the R-APS messages is the Level field. The G.8032 Ethernet Ring Protection (ERP) instance will use the configured level for sending R-APS messages, and is the level that the instance expects to receive. If the node receives an R-APS message with the improper level then the message will not be processed.

The ERP instance must be disabled to change the level, otherwise the setting is denied.

Example To set the R-APS message level field for an ERP instance named “blue” to 3, use the following commands:

```
awplus(config)# g8032 erp-instance blue
awplus(g8032-config-switch)# level 3
```

Related commands g8032 erp-instance

show g8032 erp-instance

Command changes Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

physical-ring

Overview Use this command to specify which G.8032 physical ring instance is to be used by this G.8032 Ethernet Ring Protection (ERP) instance.

Syntax

```
physical-ring <physical-ring-name>
```

Parameter	Description
<physical-ring-name>	The name of the physical ring instance.

Mode G8032 Configure Switch

Usage notes A G.8032 ERP instance in general has two ring ports, unless it is at the end of a sub-ring in which case it has only one ring port. Ring port(s) are specified using a G.8032 physical ring instance.

This command can only be accepted when the ERP instance is disabled.

Example To configure an ERP instance named “blue” to use a physical ring instance named “red”, use the following commands:

```
awplus(config)# g8032 erp-instance blue
awplus(g8032-config-switch)# physical-ring red
```

Related commands

g8032 erp-instance

g8032 physical-ring

show g8032 erp-instance

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

profile name

Overview Use this command to associate a G.8032 profile instance with this G.8032 Ethernet Ring Protection (ERP) instance.

Syntax

```
profile name <erp-profile-name>
```

Parameter	Description
<erp-profile-name>	The name of the G.8032 profile

Default If this command is not used, a profile with the name "default-profile" will be used for this G.8032 ERP instance.

Mode G8032 Configure Switch Mode

Usage notes A G.8032 ERP instance uses a profile which contains timer configurations and configurations for revertive modes of operation. This configuration can be accepted regardless of the ERP instance being disabled or enabled. Any parameters from a changed profile will take effect the next time the G.8032 state machine uses the parameters in the updated profile.

Example To associate a G.8032 profile named "prof_1" with a G.8032 ERP instance named "blue", use the following commands:

```
awplus(config)# g8032 erp-instance blue
awplus(g8032-config-switch)# profile name prof_1
```

Related commands

g8032 erp-instance

g8032 profile

show g8032 erp-instance

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

raps-channel

Overview Use this command to specify which VLAN to use as a channel for G.8032 Ring-Automatic Protection Switching (R-APS) messages sent and received by this G.8032 Ethernet Ring Protection (ERP) instance.

Use the **no** variant of this command to remove the VLAN from being used as the R-APS channel VLAN.

Syntax

```
raps-channel <vid>
no raps-channel
```

Parameter	Description
<vid>	A single VLAN-id in the range 2 to 4094.

Mode G8032 Configure Switch

Usage notes For a G.8032 ERP instance, a VLAN is used as a channel for carrying an R-APS message. This VLAN is also used to identify the proper ring instance to all the other nodes in the ring.

The VLAN must be tagged members of the G.8032 physical ring instance associated with this ERP instance. A G.8032 physical ring instance must be associated with this ERP instance. The ERP instance can not be enabled until this raps-channel VLAN has been configured properly.

The ERP instance must be disabled when using the **no** variant.

Example To configure a VLAN with a VLAN-id of "103" as a R-APS channel for an ERP instance named "blue", use the following commands:

```
awplus(config)# g8032 erp-instance blue
awplus(g8032-config-switch)# raps-channel 103
```

Related commands g8032 erp-instance

Command changes Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

service onm

Overview Use this command to enable the ONM service, which underlies CFM and G.8032.

Use the **no** version of the command to disable the unused ONM service.

Syntax

```
service onm
no service onm
```

Default Enabled

Mode Global Configuration

Usage notes Disabling the service can reduce memory usage on the switch, particularly when many VLANs are configured on ports.

Disabling the service will only take effect after you save the configuration and restart the device.

Example To disable the ONM service, use the commands:

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

Output Figure 54-1: Example output from **no service onm**

```
awplus(config)#no service onm
% Save the config and restart the device for this change to take
effect
```

Command changes Version 5.5.0-2.1: command added

rpl role

Overview Use this command to specify the role of each G.8032 Ethernet Ring Protection (ERP) ring port (also known as a link). The role can be specified as to whether it is a Ring Protection Link (RPL) or not, and if it is an RPL, whether it is the Owner or Neighbor end of an RPL.

Use the **none** variant of this command to set all the ERP instance's ring ports' RPL role to **none**.

Syntax

```
rpl role {owner|neighbor}{east-interface|west-interface|
terminating-interface}
```

```
rpl role none
```

Parameter	Description
`owner`	This sets the specified ring port to be an RPL Owner
`neighbor`	This sets the specified ring port to be an RPL Neighbor
`east-interface`	The ring port's east-interface.
`west-interface`	The ring port's west-interface.
`terminating-interface`	The ring port's terminating-interface
`none`	This sets all the ERP instance's ring ports' RPL role to none.

Default A RPL role of “none” is the default.

Mode G8032 Configure Switch

Usage notes If a node has one of its ring ports set to Owner or Neighbor, then **none** is automatically set on any other ring port as **none** is the only possible setting for the other ring port.

When using this command to set the RPL role to **none**, an interface need not be specified, as this command will set all the ring ports RPL role to **none**.

The command can only be accepted when the G.8032 ERP Instance is disabled, and the ERP instance must also have an association to a ERP Physical Ring instance.

As in the case of a sub-ring with only one physical ring port, use **terminating-interface** when specifying the RPL role as Owner or Neighbor.

Example To configure the east-interface of a ring port named “blue” to be an RPL Owner, use the following commands:

```
awplus(config)# g8032 erp-instance blue
```

```
awplus(g8032-config-switch)# rpl role owner east-interface
```

Related commands g8032 erp-instance

g8032 physical-ring

show g8032 erp-instance

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show debugging g8032

Overview Use this command to show the debugging modes enabled for G.8032.

Syntax

```
show debugging g8032
```

Mode User Exec and Privileged Exec

Example To show the debugging modes enabled for G.8032, use the following command:

```
awplus# show debugging g8032
```

Output Figure 54-2: Example output from the **show debugging g8032** command.

```
awplus#show debugging g8032
G.8032 event debugging is off
G.8032 receive debugging is off
G.8032 transmit debugging is off
```

Related commands debug g8032

undebug g8032

Command changes Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show g8032 erp-instance

Overview Use this command to show one or all G.8032 Ethernet Ring Protection (ERP) instance(s) configuration and dynamic state data.

Syntax

```
show g8032 erp-instance {<erp-instance-name>|all}
```

Parameter	Description
<erp-instance-name>	The name of a specific G.8032 ERP instance.
`all`	Use this to show all instances.

Mode User Exec and Privileged Exec

Example To show the configuration and dynamic state data for an ERP instance named "blue", use the following command:

```
awplus# show g8032 erp-instance blue
```

Output Figure 54-3: Example output from the **show g8032 erp-instance** command.

```
awplus#show g8032 erp-instance blue
------------------------------------------------------------------
Instance Name       : blue
Admin State         : enabled
G.8032 State        : IDLE
Failure of Proto-TO : false
Phy Ring            : R1 - East (port2.0.25) : West (sa1)
East Link           : Link_Unblocked
West Link           : Link_blocked
RPL Role East Link  : NONE
RPL Role West Link  : OWNER
CFM MEP East        : -
CFM MEP West        : -
ERP Profile         : default-profile
Level               : 0
Ring-ID             : 1
RAPS-Channel VLAN   : 900
Sub-ring            : disabled
Virtual Channel     : disabled
Data Traffic VLANs  : 910,920,930,940
TCN To Inst         : -
TCN Flush Event     : G8032
Wait-To-Restore     : -
Wait-To-Block       : -
NodeID              : 0000.cd37.0c25
SNMP Traps          : enabled
```

```
-----------------------------------------------------------------
          East Receiving           |           West Receiving
-----------------------------------------------------------------
Hold Off Timer      -              | Hold Off Timer      -
Signal Fail         -              | Signal Fail         -
Failure of Proto-PM false          | Failure of Proto-PM false
Version             -              | Version             -
Request             -              | Request             -
RPL-Block           -              | RPL-Block           -
DNF                 -              | DNF                 -
Block Port Ref      -              | Block Port Ref      -
NodeID              -              | NodeID              -
-----------------------------------------------------------------
           East Sending            |            West Sending
-----------------------------------------------------------------
Version             1              | Version             1
Request             NR             | Request             NR
RPL-Block           RB             | RPL-Block           RB
DNF                 1              | DNF                 1
Block Port Ref      1              | Block Port Ref      1
NodeID              0000.cd37.0c25 | NodeID         0000.cd37.0c25
-----------------------------------------------------------------
```

Table 1: Parameters in the output from the **show g8032 erp-instance** command.

Parameter	Description
Instance name	The configured <erp-instance-name> for this instance.
Admin State	The configured administrative state of this instance, either enabled or disabled. When the ERP instance is disabled, all dynamic data for other parameters in this table will be shown as "-", except for the East Link or West Link which will show the last known block or unblocked state.
G.8032 State	A dynamic parameter showing the current state of the instance per the G.8032 state machine. If the ERP Instance is disabled, it will be in the INIT state.
Phy Ring	Shows the Physical Ring Instance name that this ERP Instance is associated with along with the East/West or Terminating Interface used by the Physical Ring Instance.
East Link or West Link	A dynamic variable showing whether the instance's ring port and its VLANs are blocked or not. In the special case of an interconnection node where a sub-ring terminates, both the East Link and the West Link are the same.
RPL Role East Link or West Link	Shows the configuration of the link's role.

Table 1: Parameters in the output from the **show g8032 erp-instance** command. (cont.)

Parameter	Description
`CFM MEP East or West`	Identifies the configured MEP, if any, that is being used to provide a CFM based Signal Fail indication to this instance. The MEP is identified by its direction (Up or Down), its MEP-id, and the Maintenance Domain (MD) and Maintenance Association (MA) it is associated with by name.
`ERP Profile`	Identifies the ERP Profile instance that was configured for use by this ERP Ring instance.
`Level`	The Level that was configured for R-APS messages that are used by this ERP Ring instance.
`Ring-ID`	The Ring-ID that is to be used by this ERP instance.
`RAPS-Channel VLAN`	The VLAN-id that is configured used for sending and receiving R-APS messages for this ERP instance.
`Sub-ring`	Specifies whether the ring is operating as a Sub-ring or otherwise as a Major ring.
`Virtual Channel`	Specifies whether the sub-ring is operating with a virtual channel or not.
`Data Traffic VLANs`	A comma-separated list of configured VLAN-ids (individually, or range) that are used for data-traffic and protected by this ERP instance.
`TCN To Inst`	A comma-separated list of protocols and their instances that are to be notified when a Topology Change Notification occurs for this ERP instance. This only applies to a sub-ring with a Terminating interface and in which case "-" will be displayed if no target instances have been identified. Otherwise a "-" is displayed anyway.Identifies the protocol to notify. Only "G8032" will be supported initially.<instance-name> - Identifies the instance to notify for the given protocol.
`TCN Flush Event`	Specifies if this instance as a target instance is to send out Flush FDB messages upon TCN notifications by a detecting instance.Identifies the notifying protocol allowed. Only "G8032" will be supported initially. If no protocols have been configured then display "-".
`SNMP Traps`	Indicates whether SNMP traps have been enabled or disabled for this ERP instance.

Table 1: Parameters in the output from the **show g8032 erp-instance** command. (cont.)

Parameter	Description
`Signal Fail`	Indicates whether a Signal Fail condition is being received over the East or West ring interface. <signal-fail> consists of: "-" no Signal Fail is being indicated "Link" - indicates the interface port or LAG has gone operationally down. "CFM MEP <mep-id>" - indicates that a local CFM MEP has indicated a Signal Fail, and which MEP by mep-id.
`Failure of Protocol`	Indicates that there are defects in the receipt of an R-APS message. There are the following types: FOP-PM (Provisioning Mismatch) - "true" indicates per G.8032,that the RPL-Owner is receiving R-APS(NR,RB) messages with a node-id not of itself. In addition, since the initial implementation does not support version 1, any R-APS messages with version 1 will also indicate a FOP-PM error. The FOP-PM error can occur on an East or a West Port. FOP-TO (Time Out) - "true" indicates that a node has not received an R-APS message on any of its ring ports for 3.5 times the R-APS message interval even though one or both ring ports are capable of receiving R-APS messages (no SF, Admin Up).
`Version`	The version of the R-APS message that is being received or sent over the East or West ring interface. An R-APS message version of "1" corresponds to G.8032 version 2.
`Request`	Indicates the protection switch request being sent or received in the R-APS message. Consists of one of: NR - No Request for protection switching SF - Signal Fail MS - Manual Switch request FS - Force Switch request Event - Request a Flush to be performed. Note this is a transient condition.
`RPL Block`	Indicates whether the RPL is being blocked or not. consists of one of the following: "RB" - RPL Block is being applied by the RPL-Owner. "-" - No RPL Block is being applied by the RPL-Owner, or the R-APS message originated from a non-RPL-Owner.
`DNF`	Indicates the value of the Do Not Flush bit in the R-APS message. The value is either "0" or "1".
`Block Port Ref`	Block Port Reference refers to the node's East or West port that is being blocked and shows as "0" or "1" in accordance to G.8032.
`Node-ID`	The MAC address of this Node or the MAC address used in sending/receiving R-APS messages.

Table 1: Parameters in the output from the **show g8032 erp-instance** command. (cont.)

Parameter	Description
`East Sending or West Sending`	If this local node is not sending R-APS, then all the fields are shown as "-"
`Timers`	Wait-to-Restore - "Running" indicates this timer is active, otherwise is "-".Wait-to-Block - "Running" indicates this timer is active, otherwise is "-".Hold Off Timer - "Running" indicates this timer is active, otherwise is "-".

Related commands

data-traffic

erp-instance

g8032 erp-instance

level (g8032-switch)

physical-ring

profile name

rpl role

sub-ring

topology-change

trap (g8032-switch)

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show g8032 erp-instance statistics

Overview Use this command to show the G.8032 Ethernet Ring Protection (ERP) instance statistics.

Syntax

```
show g8032 erp-instance <erp-instance-name> statistics
```

Parameter	Description
<erp-instance-name>	The name of a specific G.8032 ERP instance

Mode User Exec and Privileged Exec

Example To show the statistics for an ERP instance named “blue”, use the following command:

```
awplus# show g8032 erp-instance blue statistics
```

Output Figure 54-4: Example output from the **show g8032 erp-instance statistics** command.

```
awplus#show g8032 erp-instance blue statistics
----------------------------------
Instance Name    : blue
Local Clear      : 0
FOP-TO           : 0
----------------------------------
 East Receiving  |  West Receiving
---------------- - ----------------
RAPS NR       15 | RAPS NR       11
RAPS NR-RB     2 | RAPS NR-RB     0
RAPS SF        0 | RAPS SF        0
RAPS FS        0 | RAPS FS        0
RAPS MS        0 | RAPS MS        0
RAPS Event     0 | RAPS Event     0
Drop Guard     0 | Drop Guard     0
Drop Error     0 | Drop Error     0
Local SF       1 | Local SF       1
FOP-PM         0 | FOP-PM         0
----------------------------------
  East Sending   |   West Sending
---------------- - ----------------
RAPS NR       17 | RAPS NR       17
RAPS NR-RB 20067 | RAPS NR-RB 20067
RAPS SF       10 | RAPS SF       10
RAPS FS        0 | RAPS FS        0
RAPS MS        0 | RAPS MS        0
RAPS Event     0 | RAPS Event     0
----------------------------------
```

Table 2: Parameters in the output from the **show g8032 erp-instance statistics** command

Parameter	Description
`Instance Name`	The configured <erp-instance-name> for this instance.
`Local clear`	The number of Clear commands invoked locally.
`FOP-TO`	The number of Failure of Protocol Time Out events seen locally.
`RAPS NR`	The number of R-APS messages with a No Request (NR) being received or sent.
`RAPS NR-RB`	The number of R-APS messages with a No Request, RPL Blocked (NR,RB) being received or sent.
`RAPS SF`	The number of R-APS messages with Signal Fail (SF) being received or sent.
`RAPS FS`	The number of R-APS messages with Forced Switch (FS) being received or sent.
`RAPS MS`	The number of R-APS messages with Manual Switch (MS) being received or sent.
`RAPS Event`	The number of R-APS messages with Event (Flush) being received or sent.
`Drop Guard`	The number of R-APS messages discarded due to Guard Timer.
`Drop Error`	The number of R-APS messages discarded due to incorrect MAC Address (unmatched Ring-ID), incorrect version, unusable Request/State, or other invalid code point in one of the message fields.
`Local SF`	The number of Signal Fail events seen locally.
`FOP-PM`	The number of Failure of Protocol events seen locally.

Related commands

clear g8032 erp-instance statistics

g8032 erp-instance

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show g8032 physical-ring

Overview Use this command to show the G.8032 physical ring instance information.

Syntax

```
show g8032 physical-ring {<physical-ring-name>|all}
```

Parameter	Description
<physical-ring-name>	The name of the physical ring
`all`	This shows all physical ring instances that have been configured

Mode User Exec and Privileged Exec

Example To show the details of a physical ring instance named “red”, use the following command:

```
awplus# show g8032 physical-ring red
```

Output Figure 54-5: Example output from the **show g8032 physical-ring** command.

```
awplus#show g8032 physical-ring red
Ring : red
====================
East     : port1.0.4
West     : port1.0.8
ERP Inst : blue
```

Table 3: Parameters in the output from the **show g8032 physical-ring** command.

Parameter	Description
`Ring`	The name of the physical ring that was configured for this physical ring instance.
`East, West, Terminating`	The physical interface port or LAG of the East or West Ring interface, or the Terminating interface that was configured for this physical ring instance.
`ERP Inst`	A comma-separated list of ERP instances by name that have been configured to use this physical ring instance, or "-" if none.

Related commands g8032 physical-ring

Command changes Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

show g8032 profile

Overview Use this command to show one specific G.8032 profile or all G.8032 profiles, and the configured information within each profile.

Syntax

```
show g8032 profile {<erp-profile-name>|default-profile|all}
```

Parameter	Description
<erp-profile-name>	The name of the G.8032 profile that was created by the user.
`default-profile`	The default name of the G.8032 profile that was created automatically by the system.
`all`	Using this will show all G.8032 profiles.

Mode User Exec and Privileged Exec

Example To show the profile details for a profile named “prof1”, use the following command:

```
awplus# show g8032 profile prof1
```

Output Figure 54-6: Example output from the **show g8032 profile** command.

```
awplus#show g8032 profile prof1
Profile : prof1
============================
Wait-To-Restore : 5 mins
Hold Off Timer  : 0 ms
Guard Timer     : 500 ms
Wait-To-Block   : 5500 ms
Protection Type : Revertive
ERP Inst        : blue
```

Table 4: Parameters in the output from **show g8032 profile** command.

Parameter	Description
`Wait-To-Restore`	The configured value in <1-12> minutes.
`Hold Off Timer`	The configured value but shown instead in milliseconds which ranges from 0 to 10,000 (10s) in 100 ms increments.
`Guard Timer`	The configured value which ranges from 10 to 2000 in 10 ms increments.

Table 4: Parameters in the output from **show g8032 profile** command. (cont.)

Parameter	Description
`Wait-To-Block`	5 seconds more than the configured Guard Time. The range is 5010 to 5200.
`ERP Inst`	Comma separated list of ERP instances using this profile, or "-" if there are none.

Related commands

enable (g8032-profile)

g8032 profile

timer (g8032-profile)

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

sub-ring

Overview Use this command to configure the mode of operation for the G.8032 Ethernet Ring Protection (ERP) instance as a sub-ring.

Use the **no** variant of this command to change the mode of operation to that of a normal fully enclosed ring.

Syntax

```
sub-ring
no sub-ring
```

Default By default the mode is **no sub-ring**.

Mode G8032 Configure Switch

Usage notes An ERP instance can operate normally as a fully enclosed ring, commonly called a major ring, or as a partially enclosed ring, called a sub-ring. Sub-rings must be attached to either a major ring (one that is fully closed) or to other sub-rings where one of the other sub-rings itself is attached to a major ring.

Setting the mode to sub-ring should also be set for all nodes in the sub-ring, as the G.8032 state machine is different from that of a major ring.

This configuration can only be accepted when the ERP instance is disabled.

When the physical ring instance used by this ERP instance is configured for terminating interface, then this ERP instance will automatically be configured to be in the sub-ring mode and can not be changed.

Example To configure an ERP instance named “blue” as a sub-ring, use the following commands:

```
awplus(config)# g8032 erp-instance blue
awplus(g8032-config-switch)# sub-ring
```

Related commands

g8032 erp-instance

g8032 physical-ring

show g8032 erp-instance

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

timer (g8032-profile)

Overview Use this command to configure a timer for a specified G.8032 Ethernet Ring Protection (ERP) instance profile.

Syntax

```
timer wait-to-restore {<1-12>|default}
timer hold-off {<0-100>|default}
timer guard-timer {<1-200>|default}
```

Parameter	Description
`wait-to-restore`	This timer is used to soak signal failure abatement to ensure the signal failure abatement is not intermittent. This timer is only used by the RPL Owner when in the revertive operation, and thus is attempting to restore the ring. It is configurable in steps of 1 to 12 minutes (default is 5 minutes).
`hold-off`	This timer allows any other underlying protection schemes to recover before G.8032 reacts to its defect as this gives time for the G.8032 defect to clear. A classic example is when the ERP Physical ring port is carried over a SONET/SDH transmission system that itself has 50ms recovery times. If G.8032 detects a failure, then increasing this timer to some value greater than 50ms would allows the SONET/SDH system to recover and have the defect that G.8032 detected disappear thus preventing the need for G.8032 to try and recover. The Hold Off timer is configurable in 0 to 10 seconds in steps of 100ms (default is 0 ms).
`guard-timer`	This is the amount of time that an ERP instance discards most R-APS messages before being allowed to process them. It is used when a clearing condition occurs yet at the same time older messages are still propagating around the ring with failure indications. For example two nodes that just noticed a link failure abatement condition could start clearing and almost immediately one of them could receive an old Signal Fail indication message from the other node (that was still in flight) which in turn causes the receiving node to react to the Signal Fail inadvertently. This timer is particularly useful where R-APS propagation time through the ring is large. Refer to ITU-T G.8032 for more information. The Guard timer is configurable in 10ms steps between 10ms and 2 seconds (default is 50 for 500ms).

Mode G8032 Profile Configuration

Example To set the wait-to-restore timer of a profile named “prof_1” to a value of 1 minute, use the following commands:

```
awplus(config)# g8032 profile prof_1
awplus(g8032-profile-config)# timer wait-to-restore 1
```

Related commands

g8032 profile

show g8032 profile

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

topology-change

Overview Use this command to enable this G.8032 Ethernet Ring Protection (ERP) instance to send a Flush Event message after notification of a Topology Change Notification (TCN) by a detecting instance.

Use the **no** variant of this command to disable the sending of the Flush Event.

Syntax

```
topology-change {g8032}
no topology-change {g8032}
```

Parameter	Description
g8032	Specify that G.8032 is the protocol that is affected by this command.

Default Topology change is enabled by default for G.8032.

Mode G8032 Configure Switch

Usage notes If this ERP instance is on an interconnecting node, then the ERP instance may need to be notified of a topology change that occurred in another G.8032 sub-ring attached to this node. The former will be termed the "target" ERP instance, and the latter the "detecting" ERP instance.

The criteria for notification is:

- the detecting ERP instance is configured as a sub-ring with a Terminating interface,
- it is protecting the same data VLANs as the target instance, and
- the target ERP instance must have two ring ports.

When the detecting ERP instance detects a topology change on its sub-ring, AlliedWare Plus™ will automatically determine which target ERP instance(s) needs to be notified. It does this by comparing the same data VLANs in the detecting ERP instance with all the other instances.

If target ERP instances are identified and these instances also have both an East and a West interface configured, then those target instances are notified. Upon notification, the target ERP instance has a couple of actions that it has to perform:

- To flush the FDB on both its East and West interfaces for the protected VLANs.
- To send out an R-APS flush event message over its East and West interfaces. The flush event message is sent around the target ring and each node on the target ring will perform an FDB flush of its protected VLANs. The sending of a R-APS flush event may not be needed in some cases and as such it is configurable.

Example To enable sending of R-APS flush event messages on an ERP instance named "blue", use the following commands:

```
awplus(config)# g8032 erp-instance blue
awplus(g8032-config-switch)# topology-change g8032
```

Related commands

g8032 erp-instance

show g8032 erp-instance

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

trap (g8032-switch)

Overview Use this command to enable or disable SNMP traps for a G.8032 Ethernet Ring Protection (ERP) instance.

Syntax

```
trap {enabled|disabled}
```

Parameter	Description
`enabled`	Enable this ERP instance to generate traps.
`disabled`	Disable this ERP instance from generating traps.

Default The SNMP traps for the ERP instance are enabled.

Mode G8032 Configure Switch

Usage notes Globally, ERP traps are disabled by default but can be enabled globally using the snmp-server enable trap command.

Example To disable the SNMP traps for an ERP instance named “blue”, use the following commands:

```
awplus(config)# g8032 erp-instance blue
awplus(g8032-config-switch)# trap disabled
```

Related commands

erp-instance

show g8032 erp-instance

snmp-server enable trap

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

undebug g8032

Overview Use this command to turn off debugging for various G.8032 debug attributes.

Syntax

```
undebug g8032 {all|event|rx|tx}
```

Parameter	Description
`all`	All G.8032 debugging
`event`	G.8032 debugging events
`rx`	G.8032 debugging Receive activities
`tx`	G.8032 debugging Transmit activities

Mode Privileged Exec

Example To turn off all G.8032 debugging, use the following command:

```
awplus# undebug g8032 all
```

Related commands

debug g8032

show debugging g8032

Command changes

Version 5.4.7-0.1: command added

Version 5.4.7-1.1: added to x310 series products

Version 5.4.7-2.1: added to x550 series products

Version 5.4.8-0.2: added to SBx8100 series products

Version 5.4.8-1.1: added to SBx908 GEN2 series products

55 Media Redundancy Protocol (MRP) Commands

Introduction

Overview This chapter provides an alphabetical list of Media Redundancy Protocol (MRP) commands.

For more information, see the MRP Feature Overview and Configuration Guide.

Command List

- "clear counter mrp" on page 2644
- "debug mrp" on page 2645
- "domain-id (mrp-ring)" on page 2646
- "domain-name (mrp-ring)" on page 2647
- "enable (mrp-ring)" on page 2648
- "lc-react" on page 2649
- "mrp ring" on page 2650
- "profile (mrp-ring)" on page 2652
- "role (mrp-ring)" on page 2653
- "service mrp" on page 2654
- "show counter mrp" on page 2655
- "show debugging mrp" on page 2659
- "show mrp ports" on page 2660
- "show mrp ring" on page 2661
- "vlan-id (mrp-ring)" on page 2663

clear counter mrp

Overview Use this command to clear the MRP counters.

Syntax

```
clear counter mrp [global|ring <ring-id>]
```

Parameter	Description
`global`	Clear only global MRP counters.
`ring`	Clear only MRP counters for a specific MRP ring.
<ring-id>	<1-65535>. The ID of an MRP ring.

Mode Privileged Exec

Example To clear all MRP counters, use the command:

```
awplus# clear counter mrp
```

To clear only the global MRP counters, use the command:

```
awplus# clear counter mrp global
```

To clear all MRP counters for MRP ring 1, use the command:

```
awplus# clear counter mrp ring 1
```

Related commands mrp ring

show counter mrp

Command changes Version 5.5.0-2.1: command added

debug mrp

Overview Use this command to enable debug output for MRP.

Use the **no** variant of this command to disable debug output.

Syntax

```
debug mrp {all|fdb|fsm|port}
no debug mrp {all|fdb|fsm|port}
```

Parameter	Description
`all`	Enable all debug output options for MRP.
`fdb`	Enable debug output for MRP forwarding database events.
`fsm`	Enable debug output for MRP state machine events.
`port`	Enable debug output for MRP port events.

Default All MRP debug output is disabled.

Mode User Exec

Usage notes Note that enabling MRP debug is not saved to the config, so enabling debug output will not be persistent.

Example To enable all MRP debug output, use the command:

```
awplus# debug mrp all
```

To disable MRP port event debug output, use the command:

```
awplus# no debug mrp port
```

Related commands mrp ring

show debugging mrp

Command changes Version 5.5.0-2.1: command added

domain-id (mrp-ring)

Overview Use this command to configure the domain ID of an MRP ring. The domain ID is used to identify the nodes in the ring, and is set in the MRP PDU packets. All nodes in an MRP ring must have the same domain ID.

Use the **no** variant of this command to reset the domain ID to the default.

Syntax

```
domain-id <uuid>
no domain-id <uuid>
```

Parameter	Description
<uuid>	A hexadecimal string that identifies the MRP ring, with a format like FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF.

Default A hexadecimal string, with the value:

FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF - <Ring ID> + 1

Mode MRP Ring Configuration

Example To configure the domain ID of MRP ring 1 to FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFF3210, use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)# domain-id
FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFF3210
```

Related commands

domain-name (mrp-ring)

enable (mrp-ring)

mrp ring

profile (mrp-ring)

role (mrp-ring)

vlan-id (mrp-ring)

Command changes Version 5.5.0-2.1: command added

domain-name (mrp-ring)

Overview Use this command to set the domain name of an MRP ring.

Use the **no** variant of this command to remove the domain name of an MRP ring.

Syntax

```
domain-name <name>
no domain-name
```

Parameter	Description
<name>	The domain name for the MRP ring.

Default No domain name is set.

Mode MRP Ring Configuration

Example To set the domain name of MRP ring 1 to 'ring1', use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)# domain-name ring1
```

To clear the domain name of MRP ring 1, use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)# no domain-name
```

Related commands

domain-id (mrp-ring)

enable (mrp-ring)

mrp ring

profile (mrp-ring)

role (mrp-ring)

vlan-id (mrp-ring)

Command changes Version 5.5.0-2.1: command added

enable (mrp-ring)

Overview Use this command to enable MRP on an MRP ring.

Use the **no** variant of this command to disable MRP on an MRP ring.

Syntax

```
enable
no enable
```

Default MRP is enabled.

Mode MRP Ring Configuration

Example To disable MRP for MRP ring 1, use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)# no enable
```

Related commands

domain-id (mrp-ring)

domain-name (mrp-ring)

mrp ring

profile (mrp-ring)

role (mrp-ring)

vlan-id (mrp-ring)

Command changes Version 5.5.0-2.1: command added

lc-react

Overview Use this command to configure the media redundancy manager (MRM) to react to MRP_LinkDown and MRP_LinkUp frames from media redundancy clients (MRCs). This may result in faster failover and recovery time.

Use the **no** variant of this command to set the MRM back to the default of ignoring those packets, and relying on the test frame interval timeout.

Syntax

```
lc-react
no lc-react
```

Default The MRM ignores MRP_LinkDown and MRP_LinkUp frames from MRCs, and relies on the test frame interval timeout.

Mode MRP Ring Manager Configuration

Example To configure MRP ring 1 to react to MRP_LinkDown and MRP_LinkUp frames, use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)# role manager
awplus(config-mrp-ring-manager)# lc-react
```

To reset MRP ring 1 to ignore MRP_LinkDown and MRP_LinkUp frames, use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)# role manager
awplus(config-mrp-ring-manager)# no lc-react
```

Related commands mrp ring

role (mrp-ring)

Command changes Version 5.5.0-2.1: command added

mrp ring

Overview Use this command to create an MRP Ring and enter MRP Ring Configuration mode, or to attach a port to an MRP ring.

In Global Configuration mode, this command will create an MRP ring and enter MRP Ring Configuration mode.

In Interface Configuration mode, this command will attach a port to an MRP ring. The MRP ring registers the port's VLAN in the MRP structure. If this is the second port to be attached to the MRP ring, it will first verify that the VLANs match.

Use the **no** variant of this command to remove a port from an MRP ring.

Syntax

```
mrp ring <ring-id>
no mrp ring <ring-id>
```

Parameter	Description
<ring-id>	<1-65535>. The ID of the MRP ring.

Mode Global Configuration mode to enter MRP Ring Configuration mode, or Interface Configuration mode to attach a port to or remove a port from an MRP ring.

Example To create MRP ring 1 and enter MRP Ring Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)#
```

To attach port1.0.1 to MRP ring 1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# mrp ring 1
```

To remove port1.0.1 from MRP ring 1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no mrp ring 1
```

Related commands

domain-id (mrp-ring)

domain-name (mrp-ring)

enable (mrp-ring)

profile (mrp-ring)

role (mrp-ring)

vlan-id (mrp-ring)

Command changes Version 5.5.0-2.1: command added

profile (mrp-ring)

Overview Use this command to set the maximum recovery timing profile for an MRP ring. This sets the worst case recovery time to 200ms or 500ms.

Use the **no** variant of this command to return to the default value (200ms).

Syntax

```
profile {200|500}
no profile
```

Parameter	Description
200	The worst-case recovery time is set to 200ms.
500	The worst-case recovery time is set to 500ms.

Default 200ms.

Mode MRP Ring Configuration

Example To configure the worst case recovery time for MRP ring 1 to 500ms, use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)# profile 500
```

To reset the worst case recovery time for MRP ring 1 to the default of 200ms, use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)# no profile
```

Related commands

domain-id (mrp-ring)

domain-name (mrp-ring)

enable (mrp-ring)

mrp ring

role (mrp-ring)

vlan-id (mrp-ring)

Command changes Version 5.5.0-2.1: command added

role (mrp-ring)

Overview Use this command to set the operating role for a node in an MRP ring. If the node is set to 'manager', it will also set the mode to MRP Ring Manager Configuration mode.

Use the **no** variant of this command to set the operating role to the default (client).

Syntax

```
role {client|manager}
no role {client|manager}
```

Parameter	Description
`client`	Assigns the operating role of media redundancy client (MRC) to the node.
`manager`	Assigns the operating role of media redundancy manager (MRM) to the node.

Default Client.

Mode MRP Ring Configuration

Example To assign the manager role to a node on MRP ring 1, use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)# role manager
awplus(config-mrp-ring-manager)#
```

To set the role of a node on MRP ring 1 to the default (client), use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)# no role
```

Related commands lc-react

mrp ring

Command changes Version 5.5.0-2.1: command added

service mrp

Overview Use this command to enable the Media Redundancy Protocol (MRP) service. This is required before any other MRP configuration can be entered. To start the MRP service, the MRP feature must be licensed.

Use the **no** variant of this command to disable the MRP service.

Syntax

```
service mrp
no service mrp
```

Default The MRP service is disabled.

Mode Global Configuration

Example To enable the MRP service, use the commands:

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

To disable the MRP service, use the commands:

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

Related commands mrp ring

Command changes Version 5.5.0-2.1: command added

show counter mrp

Overview Use this command to show the MRP counters.

The global counters provide an overall count of protocol packets being sent and received, as well as the timer and dispatcher that show the service has not halted.

The ring counters provide per-ring counters for both ring ports. These count the different types of MRP PDU packets that are sent and received. They also provide topology and port state counters that record events on the ring.

Syntax

```
show counter mrp [global|ring <ring-id>]
```

Parameter	Description
`global`	Show only global MRP counters.
`ring`	Show only MRP counters for a specific MRP ring.
<ring-id>	<1-65535>. The ID of an MRP ring.

Mode User Exec

Example To show all MRP counters, use the command:

```
awplus# show counter mrp
```

To show only the global MRP counters, use the command:

```
awplus# show counter mrp global
```

To show all MRP counters for MRP ring 1, use the command:

```
awplus# show counter mrp ring 1
```

Output Figure 55-1: Example output from **show counter mrp**

```
awplus#show counter mrp
Media Redundancy Protocol Global Counters

MRP Started             ....... 2
MRP Dispatcher          ....... 19102219
MRP Timer Tick          ....... 17373917
MRP Packet RX           ....... 1728302
MRP Packet RX Error     ....... 0
MRP Packet TX           ....... 1728303
MRP Packet TX Error     ....... 0

Media Redundancy Protocol Ring 1 Counters

Port 1 PDUs Received
MRP_Test              ......... 864150
MRP_TopologyChange    ......... 0
MRP_LinkUp            ......... 0
MRP_LinkDown          ......... 0
```

```
Port 1 PDUs Transferred
MRP_Test              ......... 864152
MRP_TopologyChange    ......... 0
MRP_LinkUp            ......... 0
MRP_LinkDown          ......... 0

Port 2 PDUs Received
MRP_Test              ......... 864152
MRP_TopologyChange    ......... 0
MRP_LinkUp            ......... 0
MRP_LinkDown          ......... 0

Port 2 PDUs Transferred
MRP_Test              ......... 864152
MRP_TopologyChange    ......... 0
MRP_LinkUp            ......... 0
MRP_LinkDown          ......... 0

Other Counters
State Changes         ......... 6
Port Blocked Set      ......... 4
Port Forwarding Set   ......... 2
Multiple Manager      ......... 0
```

Figure 55-2: Example output from **show counter mrp global**

```
awplus#show counter mrp global
Media Redundancy Protocol Global Counters

MRP Started             ....... 2
MRP Dispatcher          ....... 19211403
MRP Timer Tick          ....... 17473175
MRP Packet RX           ....... 1738228
MRP Packet RX Error     ....... 0
MRP Packet TX           ....... 1738229
MRP Packet TX Error     ....... 0
```

Figure 55-3: Example output from **show counter mrp ring 1**

```
awplus#show counter mrp ring 1
Media Redundancy Protocol Ring 1 Counters

Port 1 PDUs Received
MRP_Test              ......... 871675
MRP_TopologyChange    ......... 0
MRP_LinkUp            ......... 0
MRP_LinkDown          ......... 0

Port 1 PDUs Transferred
MRP_Test              ......... 871677
MRP_TopologyChange    ......... 0
MRP_LinkUp            ......... 0
MRP_LinkDown          ......... 0
```

```
Port 2 PDUs Received
MRP_Test               ......... 871677
MRP_TopologyChange     ......... 0
MRP_LinkUp             ......... 0
MRP_LinkDown           ......... 0

Port 2 PDUs Transferred
MRP_Test               ......... 871677
MRP_TopologyChange     ......... 0
MRP_LinkUp             ......... 0
MRP_LinkDown           ......... 0

Other Counters
State Changes          ......... 6
Port Blocked Set       ......... 4
Port Forwarding Set    ......... 2
Multiple Manager       ......... 0
```

Table 55-1: Parameters in the output from **show counter mrp**

Parameter	Description
MRP Started	The number of times the MRP service has been started with the service mrp command. This counter increases each time it is stopped and started.
MRP Dispatcher MRP Timer Tick	Internal timer tick that provides timing for the protocol and the dispatcher. This is called to process timing events, packet reception, and state changes.
MRP Packet RX	The number of MRP protocol packets received.
MRP Packet RX Error	The number of failures when receiving a packet.
MRP Packet TX	The number of MRP protocol packets sent.
MRP Packet TX Error	The number of failures when sending a packet.
MRP_Test	The number of test frames sent and received by the Media Redundancy Manager (MRM) to test if the ring is open or closed.
MRP_TopologyChange	The number of topology change frames sent from the MRM to indicate ring topology changes to Media Redundancy Clients (MRC).
MRP_LinkUp MRP_LinkDown	The number of Link Up/Down frames sent from MRC to indicate a link state change on one of its ring ports.
State Changes	The number of changes in the protocol state. These are triggered by test packets detecting the ring opening or closing, and MRP ring port link changes.
Port Blocked Set	The number of times a ring port has been set to blocking.

Table 55-1: Parameters in the output from **show counter mrp** (cont.)

Parameter	Description
Port Forwarding Set	The number of times a ring port has been set to forwarding.
Multiple Manager	A misconfiguration detected by the MRM that another manager is on the ring. This is detected from information in the MRP PDU frames.

Related commands

clear counter mrp

mrp ring

Command changes

Version 5.5.0-2.1: command added

show debugging mrp

Overview Use this command to show which debug options are enabled for MRP logging.

Syntax

```
show debugging mrp
```

Mode User Exec

Example To show the enabled MRP debugging options, use the command:

```
awplus# show debugging mrp
```

Output Figure 55-4: Example output from **show debugging mrp**

```
awplus#show debugging mrp
MRP debugging status:
  MRP Port debugging: On
  MRP FSM debugging: Off
  MRP FDB debugging: Off
```

Table 55-2: Parameters in the output from **show debugging mrp**

Parameter	Description
MRP Port debugging	Debug output for MRP port events.
MRP FSM debugging	Debug output for MRP state machine events.
MRP FDB debugging	Debug output for MRP forwarding database events.

Related commands

debug mrp

mrp ring

Command changes Version 5.5.0-2.1: command added

show mrp ports

Overview Use this command to show a summary of all ports that are configured for MRP rings.

Syntax

```
show mrp ports
```

Mode User Exec

Example To show a summary of the ports configured for MRP rings, use the command:

```
awplus# show mrp ports
```

Output Figure 55-5: Example output from **show mrp ports**

```
awplus#show mrp ports
Media Redundancy Protocol - Port Information

Connection          Port          State
-----------------------------------------
Ring 1              port1.0.23    Blocking
Ring 1              port1.0.24    Forwarding
```

Table 55-3: Parameters in the output from **show mrp ports**

Parameter	Description
Connection	The name of the MRP ring.
Port	The ID of the port.
State	The state of the port: Disabled - all packets received by the port are dropped. Blocking - all packets received by the port are dropped, with the exception of MRP protocol packets. Forwarding - all packets received by the port are forwarded.

Related commands mrp ring

Command changes Version 5.5.0-2.1: command added

show mrp ring

Overview Use this command to show the MRP ring settings for a specific ring, or for all rings.

Syntax

```
show mrp ring [<ring-id>]
```

Parameter	Description
<ring-id>	The ID of an MRP ring.

Mode Privileged Exec

Example To show the settings for all MRP rings, use the command:

```
awplus# show mrp ring
```

To show the settings for MRP ring 1, use the command:

```
awplus# show mrp ring 1
```

Output Figure 55-6: Example output from **show mrp ring**

```
awplus#show mrp ring
Media Redundancy Protocol - Ring Information
MRP Ring 1
 Domain ID:                  ffffffff-ffff-ffff-ffff-ffffffffffff
 Domain Name:
 Ring Status:                          Enabled
 Operating Mode:                       CLI
 Role:                                 Manager
 Network Status:                       Open
 Port1:                                port1.0.25
  Status:                              Forwarding
 Port2:                                port1.0.29
  Status:                              Forwarding
 Vlan ID:
 React on Link Change:                 No
 Profile:                              200ms
  Topology Change Interval:            10ms
  Topology Change Count:               3
  Short Test Frame Interval:           10ms
  Default Test Frame Interval:         20ms
  Test Monitoring Interval Count:      3
  Test Monitoring Ext Interval Count: 0
  Non-blocking MRC Supported:          No
```

Table 55-4: Parameters in the output from **show mrp ring**

Parameter	Description
Domain ID	The UUID that identifies the ring. The Domain ID is used in MRP PDU packets.
Domain Name	Description of the ring that can be set by the user.
Ring Status	Whether the ring is Enabled or Disabled.
Operating Mode	CLI - the MRP ring is configured and controlled from the command line.
Role	Whether the node is a Manager (MRM) or Client (MRC).
Network Status	Whether the MRP ring is Open or Closed (MRM only).
Port Status	The state of the port: Disabled - all packets received by the port are dropped. Blocking - all packets received by the port are dropped, with the exception of MRP protocol packets. Forwarding - all packets received by the port are forwarded.
Vlan ID	If the MRP ring is configured with a trunked VLAN, this shows the configured VLAN ID.
Profile	Whether it is configured for 200ms or 500ms.

Related commands mrp ring

Command changes Version 5.5.0-2.1: command added

vlan-id (mrp-ring)

Overview Use this command to assign a VLAN to an MRP ring.

Syntax

```
vlan-id <vlan>
```

Parameter	Description
<vlan>	<1-4094> The ID of the VLAN to be assigned.

Mode MRP Ring Configuration

Usage notes This is only possible if the ports attached to the MRP ring are set to trunked mode. In access mode, MRP will automatically set this to the VLAN of the port.

Both ports must be in the same VLAN.

Example To assign VLAN 2 to MRP ring 1, use the commands:

```
awplus# configure terminal
awplus(config)# mrp ring 1
awplus(config-mrp-ring)# vlan-id 2
```

Related commands

domain-id (mrp-ring)

domain-name (mrp-ring)

enable (mrp-ring)

mrp ring

profile (mrp-ring)

role (mrp-ring)

Command changes Version 5.5.0-2.1: command added

Part 7: Network Management

56 Allied Telesis Management Framework™ (AMF) Commands

Introduction

Overview This chapter provides an alphabetical reference for Allied Telesis Management Framework™ (AMF) commands.

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 an AMF master. See the AMF Feature Overview and Configuration Guide for information about AMF 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 262, 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 2671
- "application-proxy quarantine-vlan" on page 2672
- "application-proxy redirect-url" on page 2673
- "application-proxy threat-protection" on page 2674
- "application-proxy threat-protection send-summary" on page 2675

- "application-proxy whitelist advertised-address" on page 2676
- "application-proxy whitelist enable" on page 2677
- "application-proxy whitelist protection tls" on page 2678
- "application-proxy whitelist server" on page 2679
- "application-proxy whitelist trustpoint (deprecated)" on page 2681
- "area-link" on page 2682
- "atmf-arealink" on page 2684
- "atmf-link" on page 2686
- "atmf area" on page 2687
- "atmf area password" on page 2689
- "atmf authorize" on page 2691
- "atmf authorize provision" on page 2693
- "atmf backup" on page 2695
- "atmf backup area-masters delete" on page 2696
- "atmf backup area-masters enable" on page 2697
- "atmf backup area-masters now" on page 2698
- "atmf backup area-masters synchronize" on page 2699
- "atmf backup bandwidth" on page 2700
- "atmf backup delete" on page 2701
- "atmf backup enable" on page 2702
- "atmf backup guests delete" on page 2703
- "atmf backup guests enable" on page 2704
- "atmf backup guests now" on page 2705
- "atmf backup guests synchronize" on page 2706
- "atmf backup now" on page 2707
- "atmf backup redundancy enable" on page 2709
- "atmf backup server" on page 2710
- "atmf backup stop" on page 2712
- "atmf backup synchronize" on page 2713
- "atmf cleanup" on page 2714
- "atmf container" on page 2715
- "atmf container login" on page 2716
- "atmf controller" on page 2717
- "atmf distribute firmware" on page 2718
- "atmf domain vlan" on page 2720

- "atmf enable" on page 2723
- "atmf group (membership)" on page 2724
- "atmf guest-class" on page 2726
- "atmf log-verbose" on page 2728
- "atmf management subnet" on page 2729
- "atmf management vlan" on page 2732
- "atmf master" on page 2734
- "atmf mtu" on page 2735
- "atmf network-name" on page 2736
- "atmf provision (interface)" on page 2737
- "atmf provision node" on page 2738
- "atmf reboot-rolling" on page 2740
- "atmf recover" on page 2744
- "atmf recover guest" on page 2746
- "atmf recover led-off" on page 2747
- "atmf recover over-eth" on page 2748
- "atmf recovery-server" on page 2749
- "atmf remote-login" on page 2751
- "atmf restricted-login" on page 2753
- "atmf retry guest-link" on page 2755
- "atmf secure-mode" on page 2756
- "atmf secure-mode certificate expire" on page 2758
- "atmf secure-mode certificate expiry" on page 2759
- "atmf secure-mode certificate renew" on page 2760
- "atmf secure-mode enable-all" on page 2761
- "atmf select-area" on page 2763
- "atmf topology-gui enable" on page 2764
- "atmf trustpoint" on page 2765
- "atmf virtual-crosslink" on page 2767
- "atmf virtual-link" on page 2769
- "atmf virtual-link description" on page 2772
- "atmf virtual-link protection" on page 2773
- "atmf working-set" on page 2775
- "bridge-group" on page 2777
- "clear application-proxy threat-protection" on page 2778

- "clear atmf links" on page 2779
- "clear atmf links virtual" on page 2780
- "clear atmf links statistics" on page 2781
- "clear atmf recovery-file" on page 2782
- "clear atmf secure-mode certificates" on page 2783
- "clear atmf secure-mode statistics" on page 2784
- "clone (amf-provision)" on page 2785
- "configure boot config (amf-provision)" on page 2787
- "configure boot system (amf-provision)" on page 2789
- "copy (amf-provision)" on page 2791
- "create (amf-provision)" on page 2792
- "debug atmf" on page 2794
- "debug atmf packet" on page 2796
- "delete (amf-provision)" on page 2799
- "discovery" on page 2801
- "description (amf-container)" on page 2803
- "erase factory-default" on page 2804
- "http-enable" on page 2805
- "identity (amf-provision)" on page 2807
- "license-cert (amf-provision)" on page 2809
- "locate (amf-provision)" on page 2811
- "log event-host" on page 2813
- "login-fallback enable" on page 2814
- "modeltype" on page 2815
- "service atmf-application-proxy" on page 2816
- "show application-proxy threat-protection" on page 2817
- "show application-proxy whitelist advertised-address" on page 2819
- "show application-proxy whitelist interface" on page 2820
- "show application-proxy whitelist server" on page 2822
- "show application-proxy whitelist supplicant" on page 2823
- "show atmf" on page 2825
- "show atmf area" on page 2829
- "show atmf area guests" on page 2832
- "show atmf area guests-detail" on page 2834
- "show atmf area nodes" on page 2836

- "show atmf area nodes-detail" on page 2838
- "show atmf area summary" on page 2840
- "show atmf authorization" on page 2841
- "show atmf backup" on page 2844
- "show atmf backup area" on page 2848
- "show atmf backup guest" on page 2850
- "show atmf container" on page 2852
- "show atmf detail" on page 2855
- "show atmf group" on page 2857
- "show atmf group members" on page 2859
- "show atmf guests" on page 2861
- "show atmf guests detail" on page 2863
- "show atmf links" on page 2866
- "show atmf links detail" on page 2868
- "show atmf links guest" on page 2877
- "show atmf links guest detail" on page 2879
- "show atmf links statistics" on page 2883
- "show atmf nodes" on page 2886
- "show atmf provision nodes" on page 2888
- "show atmf recovery-file" on page 2890
- "show atmf secure-mode" on page 2891
- "show atmf secure-mode audit" on page 2893
- "show atmf secure-mode audit link" on page 2894
- "show atmf secure-mode certificates" on page 2895
- "show atmf secure-mode sa" on page 2898
- "show atmf secure-mode statistics" on page 2901
- "show atmf tech" on page 2903
- "show atmf virtual-links" on page 2906
- "show atmf working-set" on page 2908
- "show debugging atmf" on page 2909
- "show debugging atmf packet" on page 2910
- "show running-config atmf" on page 2911
- "state" on page 2912
- "switchport atmf-agentlink" on page 2914
- "switchport atmf-arealink" on page 2915

- "switchport atmf-crosslink" on page 2917
- "switchport atmf-guestlink" on page 2919
- "switchport atmf-link" on page 2921
- "type atmf node" on page 2922
- "undebug atmf" on page 2925
- "username" on page 2926

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`	Apply a Layer 2 drop for traffic generating the threat reports.
`link-down`	Set the link to error disabled in response to threats.
`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 5.4.7-2.2: command added

Version 5.4.9-0.1: **log-only** parameter 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 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 area

Overview This command creates an AMF area and gives it a name and ID number.

Use the **no** variant of this command to remove the AMF area.

This command is only valid on AMF controllers, master nodes and gateway nodes.

Syntax

```
atmf area <area-name> id <1-126> [local]
no atmf area <area-name>
```

Parameter	Description
<area-name>	The AMF area name. 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.).
<1-126>	An ID number that uniquely identifies this area.
`local`	Set the area to be the local area. The local area contains the device you are configuring.

Mode Global Configuration

Usage 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

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 2844 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 262. 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}
```

Parameter	Description
`id`	Remote server backup server identifier.
`{1|2}`	The backup server identifier number (1 or 2). Note that there can be up to two backup servers, numbered 1 and 2 respectively, and you would need to run this command separately for each server.
<hostlocation>	Either the name or the IP address (IPv4 or IPv6) of the selected backup server (1 or 2).
`username`	Configure the username to log in with on the selected remote file server.
<username>	The selected remote file server's username.
`path`	The location of the backup files on the selected remote file server. By default this will be the home directory of the username used to log in with.
<path>	The directory path utilized to store the backup files on the selected remote file server. No spaces are allowed in the path.
`port`	The connection to the selected remote backup file server using SSH. By default SSH connects to a device on TCP port 22 but this can be changed with this command.
`<1-65535>`	A TCP port within the specified range.

Defaults Remote backup servers are not configured. The default SSH TCP port is 22. The path utilized on the remote file server is the home directory of the username.

Mode Global Exec

Usage notes The hostname and username parameters must both be configured.

Examples To configure server 1 with an IPv4 address and a username of *backup1*, use the commands:

```
AMF_Master_1# configure terminal
```

```
AMF_Master_1(config)# atmf backup server id 1 192.168.1.1
username backup1
```

To configure server 1 with an IPv6 address and a username of *backup1*, use the command:

```
AMF_backup1_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 FFEE::01 username backup1
```

To configure server 2 with a hostname and username, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com username backup2
```

To configure server 2 with a hostname and username in addition to the optional path and port parameters, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com username backup2 path tokyo port 1024
```

To unconfigure the AMF remote backup file server 1, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# no atmf backup server id 1
```

Related commands show atmf backup

atmf backup stop

Overview Running this command stops a backup that is currently running on the master node you are logged onto. Note that if you have two masters and want to stop both, then you can either run this command separately on each master node, or add both masters to a working set, and issue this command to the working set.

Note that this command can only be run on a master node.

Syntax

```
atmf backup stop
```

Mode Privileged Exec

Usage notes This command is used to halt an AMF backup that is in progress. In this situation the backup process will finish on its current node and then stop.

Example To stop a backup that is currently executing on master node node-1, use the following command:

```
AMF_Master_1# amf backup stop
```

Related commands

atmf backup

atmf backup enable

atmf backup now

show atmf backup

atmf backup synchronize

Overview For the master node you are connected to, this command initiates a system backup of files from the node's active remote file server to its backup remote file server. Note that this process happens automatically each time the network is backed up.

Note that this command can only be run from a master node.

Syntax

```
atmf backup synchronize
```

Mode Privileged Exec

Example When connected to the master node AMF_Master_1, the following command will initiate a backup of all system related files from its active remote file server to its backup remote file server.

```
AMF_Master_1# atmf backup synchronize
```

Related commands

atmf backup enable

atmf backup redundancy enable

show atmf

show atmf backup

atmf cleanup

Overview This command is an alias to the erase factory-default command.

atmf container

Overview Use this command to create or update an AMF container on a Virtual AMF Appliance (VAA) virtual machine.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the AMF Feature Overview and Configuration Guide for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove an AMF container.

Syntax

```
atmf container <container-name>
no atmf container <container-name>
```

Parameter	Description
<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

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

http-enable

username

modeltype

switchport atmf-guestlink

show atmf links guest

show atmf guests

login-fallback enable

atmf log-verbose

Overview This command limits the number of log messages displayed on the console or permanently logged.

Use the **no** variant of this command to reset to the default.

Syntax

```
atmf log-verbose <1-3>
no atmf log-verbose
```

Parameter	Description
<1-3>	The verbose limitation (3 = noisiest, 1 = quietest)

Default The default log display is 3.

Usage This command is intended for use in large networks where verbose output can make the console unusable for periods of time while nodes are joining and leaving.

Mode Global Configuration

Example To set the log-verbose to noise level 2, use the command:

```
node-1# configure terminal
node-1(config)# atmf log-verbose 2
```

Validation Command show atmf

atmf management subnet

Overview This command is used to assign a subnet that will be allocated to the AMF management and domain management VLANs. From the address space defined by this command, two subnets are created, a management subnet component and a domain component, as explained in the Usage section below.

AMF uses these internal IPv4 subnets to communicate network status information between nodes. These subnet addresses must be reserved for AMF and not used for other purposes.

CAUTION: *Every member of your AMF network must have the same domain VLAN, management VLAN, and management subnet.*

CAUTION: *If you change the domain VLAN, management VLAN, or management subnet of a node, that change takes effect immediately and the node will immediately leave the AMF network and try to rejoin it. The AMF network will not be complete until you have given all devices the same setting, so they can all rejoin the AMF network.*

Use the **no** variant of this command to remove the assigned subnet.

Syntax

```
atmf management subnet <a.b.0.0>
no atmf management subnet
```

Parameter	Description
<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 card:/5.4.6/x*-5.4.6-*.rel will select from the folder card:/5.4.6 the latest file that matches the selection x (wildcard) -5.4.6-(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 x510 nodes in an AMF network, use the following command:

```
Bld2_Floor_1# atmf working-set group x510
```

This command returns the following type of screen output:

```
====================
node1, node2, node3:
====================

Working set join

AMF_NETWORK[3]#
```

```
ATMF_NETWORK[3]# atmf reboot-rolling
```

When the reboot has completed, a number of status screens appear. The selection of these screens will depend on the parameters set.

```
Bld2_Floor_1#atmf working-set group x510

============================
SW_Team1, SW_Team2, SW_Team3:
============================

Working set join

ATMF_NETWORK[3]#atmf reboot-rolling
ATMF Rolling Reboot Nodes:

                    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 releases, use the following command:

```
Node_1# atmf working-set group all

ATMF_NETWORK[9]# atmf reboot-rolling
card:/5.4.6/x*-5.4.6-*.rel
```

```
ATMF Rolling Reboot Nodes:

                    Timeout
Node Name           (Minutes)    New Release File             Status
-------------------------------------------------------------------------
SW_Team1               8         x510-5.4.6-0.1.rel           Release Ready
SW_Team2              10         x510-5.4.6-0.1.rel           Release Ready
SW_Team3               8         ---                          Not Supported
HW_Team1               6         ---                          Incompatible
Bld1_Floor_2           2         x930-5.4.6-0.1.rel           Release Ready
Bld1_Floor_1           4         ---                          Incompatible
Building_1             2         ---                          Incompatible
Building_2             2         x908-5.4.6-0.1.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 aaa authentication auth-web

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.

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>
```
```
no atmf virtual-crosslink id <local-id>
```

Parameter	Description
<local-id>	ID of the local tunnel port, a value between 1 and 4094.
<local-ip>	IPv4 address of the local tunnel port in a.b.c.d format.
<remote-id>	ID of the remote tunnel port, a value between 1 and 4094.
<remote-ip>	IPv4 address of the remote tunnel port in a.b.c.d format.

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. 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 5.4.7-0.3: 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.

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>]

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-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. 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.

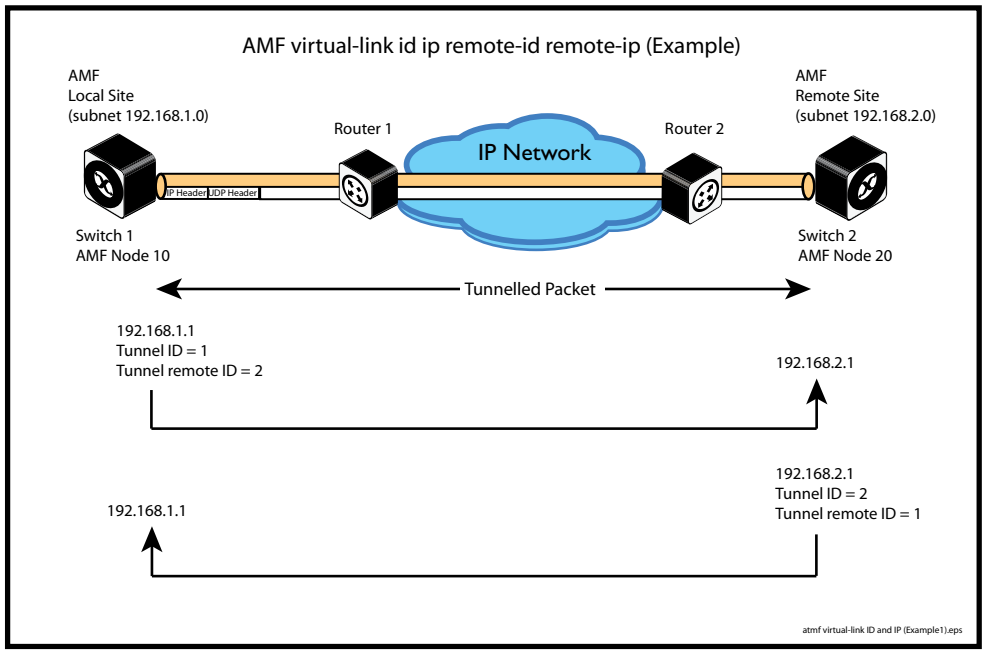
For instructions on how to configure dynamic IP addresses on virtual-links, see the AMF Feature Overview and Configuration Guide.

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 56-1: 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 5.4.9-0.1: **interface** parameter added

atmf virtual-link description

Overview Use this command to add a description to an existing AMF virtual-link.

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.

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 The following limitations need to be considered when creating secure virtual-links.

- 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.

Secure virtual-links are only supported on the following device listed in the table below. There is also a limit to the number of links these devices support.

Device	Virtual-link Limit
AMF Cloud/ VAA	300
AR4050S AR3050S AR2050V AR2010V	60
x220 x230/x230L x310 x510/x510L IX5-28GPX	2

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
```

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

Overview Use this command to connect an AMF container to a bridge created on a Virtual AMF Appliance (VAA) virtual machine. This allows the AMF container to connect to a physical network.

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 create a bridge group for AMF container “vac-wlg-1” and , 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 56-2: 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 56-3: 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 56-4: 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 56-5: 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 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 2925.*

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
```

This example applies the **debug atmf packet** command and combines many of its options:

```
node_1# debug atmf packet direction rx level 1 num-pkts 60
filter node x930 interface port1.0.1 pkt-type 4 7 10
```

delete (amf-provision)

Overview This command deletes files that have been created for loading onto a provisioned node. It can only be run on master nodes.

Syntax

```
delete
```

Mode AMF Provisioning

Usage notes This command is only available on master nodes in the AMF network. The command will only work if the provisioned node specified in the command has already been set up (although the device itself is still yet to be installed). Otherwise, an error message is shown when the command is run.

You may want to use the **delete** command to delete a provisioned node that was created in error or that is no longer needed.

This command cannot be used to delete backups created by the AMF backup procedure. In this case, use the command atmf backup delete to delete the files.

NOTE: *This command allows provisioned entries to be deleted even if they have been referenced by the atmf provision (interface) command, so take care to only delete unwanted entries.*

Example To delete backup files for a provisioned node named device3 use the command:

```
device1# atmf provision node device3
device1(atmf-provision)# delete
```

To confirm that the backup files for provisioned node device3 have been deleted use the command:

```
device1# show atmf backup
```

The output should show that the provisioned node device3 no longer exists in the backup file, as shown in the figure below:

Figure 56-6: 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 two internally defined discovery methods: static or dynamic.

With dynamic learning (the default method), AMF learns IP address and MAC addresses of guest nodes from LLDP or DHCP snooping. Dynamic learning is only supported when using IPv4. For IPv6, use static learning.

With dynamic learning, ensure that the command ip dhcp snooping delete-by-linkdown is set.

With static learning, you use 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.

The **no** variant of this command returns the discovery method to **dynamic**.

Syntax

```
discovery [static|dynamic]
no discovery
```

Parameter	Description
`static`	Statically assigned.
`dynamic`	Learned from DCHCP Snooping or LLDP.

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 the discovery of the guest-class camera to operate statically, 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 TQ4600-1 to its default of **dynamic**, use the following commands:

```
Node1# configure terminal
Node1(config)# atmf guest-class TQ4600-1
Node1(config-atmf-guest)# no discovery
```

Related commands

atmf guest-class

switchport atmf-guestlink

show atmf links guest

show atmf nodes

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

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 56-7: 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 56-8: 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 56-9: 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 56-1: 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 56-10: 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 static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • 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 56-11: 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 56-12: 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 static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • 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 56-13: 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 57: 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 58: 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 59: 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 60: 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 60: 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 61: 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 62: 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 63: 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 64: 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 56-14: 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 65: 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 56-15: 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 66: 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 67: 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 68: 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 68: 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 69: 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 70: 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 71: 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 56-16: 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 56-1: 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 56-17: 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 56-2: 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 56-18: 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 56-3: 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 56-4: 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 56-5: 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 56-6: 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 56-7: 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 57: 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. This will be one of USB, SD, or NONE. 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 57: 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 58: 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 56-19: 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 56-1: 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 56-20: 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 56-21: 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 56-2: 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 56-22: 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 56-3: 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 56-3: 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

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 57: 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 2775. This can be seen from the network level prompt, which in this case is *AMF_NETWORK[6]#*.

Table 58: 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 59: 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 60: 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 61: 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 56-23: 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 62: 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 62: 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 56-24: 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 63: 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 56-25: 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 56-1: 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 56-1: 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 57: 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 57: 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 57: 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 57: 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 57: 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 58: 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 58: 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 58: 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 56-26: 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 56-1: 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 56-1: 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

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 56-27: 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 56-2: 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 56-2: 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 56-2: 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

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 57: 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 57: 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 56-28: 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 56-29: 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 56-1: 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 57: 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 56-1: 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 56-30: 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 56-31: 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 56-32: 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 56-33: 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 56-2: 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 56-34: 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 56-3: 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 56-35: 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 56-4: 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 56-36: 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 56-5: 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 56-37: 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 56-6: 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 56-38: 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 56-39: 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 56-7: 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 56-40: 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 56-41: 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 57: 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 57: 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 58: 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 58: 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 56-1: 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 56-2: 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 56-3: 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 56-4: 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 57: 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 56-1: 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 56-2: 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.

Use the **no** variant of this command to remove any crosslink that may exist for the selected port or aggregated link.

Syntax

```
switchport atmf-crosslink
no switchport atmf-crosslink
```

Mode Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

Usage notes Crosslinks can be used anywhere within an AMF network. They have the effect of separating the AMF network into separate domains.

Where this command is used, it is also good practice to use the **switchport trunk native vlan** command with the parameter **none** selected. This is to prevent a network storm on a topology of ring connected devices.

Example 1 To make switchport port1.0.1 an AMF crosslink, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# switchport atmf-crosslink
```

Example 2 This example is shown twice. Example 2A is the most basic command sequence. Example 2B is a good practice equivalent that avoids problems such as broadcast storms that can otherwise occur.

Example 2A To make static aggregator sa1 an AMF crosslink, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface sa1
Node_1(config-if)# switchport atmf-crosslink
```

Example 2B To make static aggregator sa1 an AMF crosslink, use the following commands for good practice:

```
Node_1# configure terminal
Node_1(config)# interface sa1
Node_1(config-if)# switchport atmf-crosslink
Node_1(config-if)# switchport trunk allowed vlan add 2
Node_1(config-if)# switchport trunk native vlan none
```

In this example VLAN 2 is assigned to the static aggregator, and the native VLAN (VLAN 1) is explicitly excluded from the aggregated ports and the crosslink assigned to it.

NOTE: *The AMF management and domain VLANs are automatically added to the aggregator and the crosslink.*

Related commands show atmf links statistics

switchport atmf-guestlink

Overview Guest links are used to provide basic AMF functionality to non AMF capable devices. Guest links can be configured for either a selected switch port or a range of switch ports and use generic protocols to collect status and configuration information that the guest devices make available.

Use the **no** variant of this command to remove the guest node functionality from the selected port or ports.

NOTE: *AMF guest nodes are not supported on ports using the OpenFlow protocol.*

Syntax

```
switchport atmf-guestlink [class <guest-class>] [ip <A.B.C.D>|
ipv6 <X:X::X:X>]
no switchport atmf-guestlink
```

Parameter	Description
`class`	Set a guest class
`<guest-class>`	The name of the guest class.
`ip`	Specifies that the address following will have an IPv4 format
`<A.B.C.D>`	The guest node's IP address in IPv4 format.
`ipv6`	Specifies that the address following will have an IPv6 format
`<X:X::X:X>`	The guest node's IP address in IPv6 format.

Default No guest links are configured.

Mode Interface

Example 1 To configure switchport port1.0.1 to be a guest link, that will connect to a guest node having a guest class of **camera** and an IPv4 address of **192.168.3.3**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink class camera ip
192.168.3.3
```

Example 2 To configure switchport port1.0.1 to be a guest link, which will connect to a guest node having a guest class of **phone** and an IPv6 address of **2001:db8:21e:10d::5**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink class phone ipv6
2000:db8:21e:10d::5
```

Example 3 To configure switchport port1.0.1 to be a guest link, using the default model type and learning method address, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink
```

Example 4 To configure switchports port1.0.1 to port1.0.3 to be guest links, for the guest class **camera**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1-port1.0.3
node1(config-if)# switchport atmf-guestlink class camera
```

Example 5 To remove the guest-link functionality from switchport port1.0.1, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# no switchport atmf-guestlink
```

Related commands

atmf guest-class

discovery

http-enable

username

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 node

Overview This command configures a trigger to be activated at an AMF node join event or leave event.

Syntax

```
type atmf node {join|leave}
```

Parameter	Description
join	AMF node join event.
leave	AMF node leave event.

Mode Trigger Configuration

CAUTION: *Only configure this trigger on one device because it is a network wide event.*

Example 1 To configure trigger 5 to activate at an AMF node leave event, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger) type atmf node leave
```

Example 2 The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
====================
node1, node2, node3:
====================

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=======
node1:
========

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
001 Periodic (2 min)   Periodic Status Chk  Y  N  Y Continuous  1   smtwtfs
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------

==============
Node2, Node3,
==============

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------
```

Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
========
Node1:
========

trigger 1
 type periodic 2
 script 1 atmf.scp
trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!

============
Node2, Node3:
============

trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!
```

Related commands show trigger

undebug atmf

Overview This command is an alias for the **no** variant of the debug atmf command.

username

Overview This command enables you to assign a **username** to a guest class. Guests may require a username and possibly also a password. In its non-encypted form the password must be between 1 and 32 characters and will allow spaces. In its encrypted form the password must be between 1 to 64 characters and will allow any character

Syntax

```
username <name> password [8] <userpass>
no username
```

Parameter	Description
`username`	Indicates that a user name is to follow.
<name>	User name of the guest node.
`password`	Indicates that a password (or specifier) is to follow.
`8`	Specifier indicating that the following password is encrypted. It's primary purpose is to differentiate between the configuration input and the CLI input. You should not specify this for CLI input.
<userpass>	The password to be entered for the guest node.

Default No usernames 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

57 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

- "bootfile" on page 2929
- "clear ip dhcp binding" on page 2930
- "default-router" on page 2931
- "dns-server" on page 2932
- "domain-name" on page 2933
- "host (DHCP)" on page 2934
- "ip address dhcp" on page 2935
- "ip dhcp bootp ignore" on page 2937
- "ip dhcp leasequery enable" on page 2938
- "ip dhcp option" on page 2939
- "ip dhcp pool" on page 2941
- "ip dhcp-client default-route distance" on page 2942
- "ip dhcp-client request vendor-identifying-specific" on page 2944
- "ip dhcp-client vendor-identifying-class" on page 2945
- "ip dhcp-relay agent-option" on page 2946
- "ip dhcp-relay agent-option checking" on page 2948
- "ip dhcp-relay agent-option remote-id" on page 2949

- "ip dhcp-relay information policy" on page 2950
- "ip dhcp-relay maxhops" on page 2952
- "ip dhcp-relay max-message-length" on page 2953
- "ip dhcp-relay server-address" on page 2955
- "ip dhcp-relay use-client-side-address" on page 2957
- "lease" on page 2959
- "network (DHCP)" on page 2961
- "next-server" on page 2962
- "option" on page 2963
- "probe enable" on page 2965
- "probe packets" on page 2966
- "probe timeout" on page 2967
- "probe type" on page 2968
- "range" on page 2969
- "route" on page 2970
- "service dhcp-relay" on page 2971
- "service dhcp-server" on page 2972
- "short-lease-threshold" on page 2973
- "show counter dhcp-client" on page 2975
- "show counter dhcp-relay" on page 2976
- "show counter dhcp-server" on page 2979
- "show dhcp lease" on page 2981
- "show ip dhcp binding" on page 2982
- "show ip dhcp pool" on page 2983
- "show ip dhcp-relay" on page 2988
- "show ip dhcp server statistics" on page 2989
- "show ip dhcp server summary" on page 2991
- "subnet-mask" on page 2992

bootfile

Overview This command sets the boot filename for a DHCP server pool. This is the name of the boot file that the client should use in its bootstrap process. It may need to include a path.

The **no** variant of this command removes the boot filename from a DHCP server pool.

Syntax

```
bootfile <filename>
no bootfile
```

Parameter	Description
<filename>	The boot file name.

Mode DHCP Configuration

Example To configure the boot filename for a pool `P2`, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# bootfile boot/main_boot.bt
```

clear ip dhcp binding

Overview This command clears either a specific lease binding or the lease bindings specified by the command or DHCP server. The command will only take effect on dynamically allocated bindings, not statically configured bindings.

Syntax

```
clear ip dhcp binding {ip <ip-address>|mac
<mac-address>|all|pool <pool-name>|range <low-ip-address>
<high-ip-address>}
```

Parameter	Description
`ip <ip-address>`	IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D.
`mac <mac-address>`	MAC address of the DHCP client, in hexadecimal notation in the format HHHH.HHHH.HHHH.
`all`	All DHCP bindings.
`pool <pool-name>`	Description used to identify DHCP server address pool. Valid characters are any printable character. If the name contains spaces then you must enclose these in “quotation marks”.
`range<low-ip-address> <high-ip-address>`	IPv4 address range for DHCP clients, in dotted decimal notation. The first IP address is the low end of the range, the second IP address is the high end of the range.

Mode User Exec and Privileged Exec

Usage A specific binding may be deleted by **ip** address or **mac** address, or several bindings may be deleted at once using **all**, **pool** or **range**.

Note that if you specify to clear the **ip** or **mac** address of what is actually a static DHCP binding, an error message is displayed. If **all**, **pool** or **range** are specified and one or more static DHCP bindings exist within those addresses, any dynamic entries within those addresses are cleared but any static entries are not cleared.

Examples To clear the specific IP address binding `192.168.1.1`, use the command:

```
awplus# clear ip dhcp binding ip 192.168.1.1
```

To clear all dynamic DHCP entries, use the command:

```
awplus# clear ip dhcp binding all
```

Related commands show ip dhcp binding

default-router

Overview This command adds a default router to the DHCP address pool you are configuring. You can use this command multiple times to create a list of default routers on the client's subnet. This sets the router details using the pre-defined option 3. Note that if you add a user-defined option 3 using the **option** command, then you will override any settings created with this command.

The **no** variant of this command removes either the specified default router, or all default routers from the DHCP pool.

Syntax

```
default-router <ip-address>
no default-router [<ip-address>]
```

Parameter	Description
<ip-address>	IPv4 address of the default router, in dotted decimal notation.

Mode DHCP Configuration

Examples To add a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# default-router 192.168.1.2
```

To remove a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router 192.168.1.2
```

To remove all routers from the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router
```

dns-server

Overview This command adds a Domain Name System (DNS) server to the DHCP address pool you are configuring. You can use this command multiple times to create a list of DNS name servers available to the client. This sets the DNS server details using the pre-defined option 6.

The **no** variant of this command removes either the specified DNS server, or all DNS servers from the DHCP pool.

Syntax

```
dns-server <ip-address>
no dns-server [<ip-address>]
```

Parameter	Description
<ip-address>	IPv4 address of the DNS server, in dotted decimal notation.

Mode DHCP Configuration

Examples To add the DNS server with the assigned IP address 192.168.1.1 to the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# dns-server 192.168.1.1
```

To remove the DNS server with the assigned IP address 192.168.1.1 from the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no dns-server 192.168.1.1
```

To remove all DNS servers from the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no dns-server
```

Related commands default-router

show ip dhcp pool

subnet-mask

domain-name

Overview This command adds a domain name to the DHCP address pool you are configuring. Use this command to specify the domain name that a client should use when resolving host names using the Domain Name System. This sets the domain name details using the pre-defined option 15.

Note that if you add a user-defined option 15 using the option command, then you will override any settings created with this command.

The **no** variant of this command removes the domain name from the address pool.

Syntax

```
domain-name <domain-name>
no domain-name
```

Parameter	Description
<domain-name>	The domain name you wish to assign the DHCP pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".

Mode DHCP Configuration

Examples To add the domain name `Nerv_Office` to DHCP pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# domain-name Nerv_Office
```

To remove the domain name `Nerv_Office` from DHCP pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no domain-name Nerv_Office
```

Related commands

default-router

dns-server

option

service dhcp-server

show ip dhcp pool

subnet-mask

host (DHCP)

Overview This command adds a static host address to the DHCP address pool you are configuring. The client with the matching MAC address is permanently assigned this IP address. No other clients can request it.

The **no** variant of this command removes the specified host address from the DHCP pool. Use the **no host all** command to remove all static host addresses from the DHCP pool.

Syntax

```
host <ip-address> <mac-address>
no host <ip-address>
no host all
```

Parameter	Description
<ip-address>	IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D
<mac-address>	MAC address of the DHCP client, in hexadecimal notation in the format HHHH.HHHH.HHHH

Mode DHCP Configuration

Usage Note that a network/mask must be configured using a **network** command before issuing a **host** command. Also note that a host address must match a network to add a static host address.

Examples To add the host at `192.168.1.5` with the MAC address `000a.451d.6e34` to DHCP pool `1`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool 1
awplus(dhcp-config)# network 192.168.1.0/24
awplus(dhcp-config)# host 192.168.1.5 000a.451d.6e34
```

To remove the host at `192.168.1.5` with the MAC address `000a.451d.6e34` from DHCP pool `1`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool 1
awplus(dhcp-config)# no host 192.168.1.5 000a.451d.6e34
```

Related Commands show ip dhcp pool

ip address dhcp

Overview This command activates the DHCP client on the interface you are configuring. This allows the interface to use the DHCP client to obtain its IP configuration details from a DHCP server on its connected network.

The **client-id** and **hostname** parameters are identifiers that you may want to set in order to interoperate with your existing DHCP infrastructure. If neither option is needed, then the DHCP server uses the MAC address field of the request to identify the host.

The DHCP client supports the following IP configuration options:

- Option 1— the subnet mask for your device.
- Option 3— a list of default routers.
- Option 6 — a list of DNS servers. This list appends the DNS servers set on your device with the ip name-server command.
- Option 15—a domain name used to resolve host names. This option replaces the domain name set with the ip domain-name command. Your device ignores this domain name if it has a domain list set using the ip domain-list command.
- Option 51—lease expiration time.

The **no** variant of this command stops the interface from obtaining IP configuration details from a DHCP server.

Syntax

```
ip address dhcp [client-id <interface>] [hostname <hostname>]
no ip address dhcp
```

Parameter	Description
`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 a VLAN interface or a local loopback interface.

Examples To set the interface vlan2 to use DHCP to obtain an IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip address dhcp
```

To stop the interface vlan2 from using DHCP to obtain its IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip address dhcp
```

Related commands

ip address (IP Addressing and Protocol)

show ip interface

show running-config

ip dhcp bootp ignore

Overview This command configures the DHCP server to ignore any BOOTP requests it receives. The DHCP server accepts BOOTP requests by default.

The **no** variant of this command configures the DHCP server to accept BOOTP requests. This is the default setting.

Syntax

```
ip dhcp bootp ignore
no ip dhcp bootp ignore
```

Mode Global Configuration

Examples To configure the DHCP server to ignore BOOTP requests, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp bootp ignore
```

To configure the DHCP server to respond to BOOTP requests, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp bootp ignore
```

Related commands show ip dhcp server summary

ip dhcp leasequery enable

Overview Use this command to enable the DHCP server to respond to DHCPLEASEQUERY packets. Enabling the DHCP leasequery feature allows a DHCP Relay Agent to obtain IP address information directly from the DHCP server using DHCPLEASEQUERY messages.

Use the **no** variant of this command to disable the support of DHCPLEASEQUERY packets.

For more information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp leasequery enable
no ip dhcp leasequery enable
```

Default DHCP leasequery support is disabled by default.

Mode Global Configuration

Examples To enable DHCP leasequery support, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp leasequery enable
```

To disable DHCP leasequery support, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp leasequery enable
```

Related commands

show counter dhcp-server

show ip dhcp server statistics

show ip dhcp server summary

ip dhcp option

Overview This command creates a user-defined DHCP option. Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

The **no** variant of this command removes either the specified user-defined option, or removes all user-defined options. This also automatically removes the user-defined options from the associated DHCP address pools.

Syntax

```
ip dhcp option <1-254> [name <option-name>] [<option-type>]
no ip dhcp option [<1-254>|<option-name>]
```

Parameter	Description	
<1-254>	The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.	
<option-name>	Option name used to identify the option. You cannot use a number as the option name. Valid characters are any printable character. If the name contains spaces then you must enclose it in “quotation marks”. Default: no default	
<option-type>	The option value. You must specify a value that is appropriate to the option type:	
	`asci`	An ASCII text string
	`hex`	A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.
	`ip`	An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually by using the option command multiple times.
	`integer`	A number from 0 to 4294967295.
	`flag`	A value that either sets (to 1) or unsets (to 0) a flag: **true**, **on**, or **enabled** will set the flag. **f alse**, **off** or **disabled** will unset the flag.

Mode Global Configuration

Examples To define a user-defined ASCII string option as option 66, without a name, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp option 66 ascii
```

To define a user-defined hexadecimal string option as option 46, with the name "tcpip-node-type", use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp option 46 name tcpip-node-type hex
```

To define a user-defined IP address option as option 175, with the name `special-address`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp option 175 name special-address ip
```

To remove the specific user-defined option with the option number `12`, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option 12
```

To remove the specific user-defined option with the option name `perform-router-discovery`, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option perform-router-discovery
```

To remove all user-defined option definitions, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option
```

Related commands

default-router

dns-server

domain-name

show ip dhcp server summary

subnet-mask

ip dhcp pool

Overview This command will enter the configuration mode for the pool name specified. If the name specified is not associated with an existing pool, the device will create a new pool with this name, then enter the configuration mode for the new pool.

Once you have entered the DHCP configuration mode, all commands executed before the next **exit** command will apply to this pool.

You can create multiple DHCP pools on devices with multiple interfaces. This allows the device to act as a DHCP server on multiple interfaces to distribute different information to clients on the different networks.

The **no** variant of this command deletes the specific DHCP pool.

Syntax

```
ip dhcp pool <pool-name>
no ip dhcp pool <pool-name>
```

Parameter	Description
<pool-name>	Description used to identify this DHCP pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in “quotation marks”.

Mode Global Configuration

Example To create the DHCP pool named `P2` and enter DHCP Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)#
```

To delete the DHCP pool named `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp pool P2
```

Related commands service dhcp-server

ip dhcp-client default-route distance

Overview Use this command to specify an alternative Administrative Distance (AD) for the current default route (from DHCP) for an interface.

Use the **no** variant of this command to set the AD back to the default of 1.

Syntax

```
ip dhcp-client default-route distance [<1-255>]
no ip dhcp-client default-route distance
```

Parameter	Description
<1-255>	Administrative Distance (AD) from the range 1 though 255.

Default 1

Mode Interface Configuration for a VLAN interface or a local loopback interface.

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, such as an interface with lower bandwidth or a particular role like the management interface.

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 configure vlan10 as a DHCP client and to set the AD for the default route added by DHCP to 150, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# ip address dhcp
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 vlan10
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

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 vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-client request
vendor-identifying-specific
```

To remove the vendor-identifying-specific request on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
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

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 vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-client vendor-identifying-class
```

Related commands ip address dhcp

ip dhcp-client request vendor-identifying-specific

Command changes Version 5.4.7-2.1: command added

ip dhcp-relay agent-option

Overview This command enables the DHCP Relay Agent to insert the DHCP Relay Agent Information Option (Option 82) into the client-request packets that it relays to its DHCP server. This allows the DHCP Relay Agent to pass on information to the server about the network location of the client device. The DHCP Relay Agent strips the DHCP Relay Agent Option 82 field out of the DHCP server's response, so that the DHCP client never sees this field.

When the DHCP Relay Agent appends its DHCP Relay Agent Option 82 data into the packet, it first overwrites any pad options present; then if necessary, it increases the packet length to accommodate the DHCP Relay Agent Option 82 data.

The **no** variant of this command stops the DHCP Relay Agent from appending the Option 82 field onto DHCP requests before forwarding it to the server.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

NOTE: *The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands ip dhcp-relay agent-option and ip dhcp-relay information policy have been configured.*

Syntax

```
ip dhcp-relay agent-option
no ip dhcp-relay agent-option
```

Default DHCP Relay Agent Information Option (Option 82) insertion is disabled by default.

Mode Interface Configuration for a VLAN interface.

Usage notes Use this command to alter the DHCP Relay Agent Option 82 setting when your device is the first hop for the DHCP client. To limit the maximum length of the packet, use the ip dhcp-relay max-message-length command.

This command cannot be enabled if DHCP snooping is enabled on your device (service dhcp-snooping command), and vice versa.

Examples To make the DHCP Relay Agent listening on vlan2 append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the DHCP Relay Agent from appending the DHCP Relay Agent Option 82 field on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay agent-option
```

Related commands

ip dhcp-relay agent-option remote-id

ip dhcp-relay information policy

ip dhcp-relay max-message-length

service dhcp-relay

ip dhcp-relay agent-option checking

Overview

This command enables the DHCP Relay Agent to check DHCP Relay Agent Information Option (Option 82) information in response packets returned from DHCP servers. If the information does not match the information it has for its own client (downstream) interface then the DHCP Relay Agent drops the packet. Note that ip dhcp-relay agent-option must be configured.

The DHCP Relay Agent Option 82 field is included in relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled (ip dhcp-relay agent-option), and
- DHCP Relay Agent is enabled on the device (service dhcp-relay)

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay agent-option checking
no ip dhcp-relay agent-option checking
```

Mode

Interface Configuration for a VLAN interface.

Examples

To make the DHCP Relay Agent listening on vlan2 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay agent-option
awplus(config-if)# ip dhcp-relay agent-option checking
```

To stop the DHCP Relay Agent on vlan2 from checking the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay agent-option checking
```

Related commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option remote-id

ip dhcp-relay information policy

service dhcp-relay

ip dhcp-relay agent-option remote-id

Overview Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field the DHCP Relay Agent inserts into clients' request packets. The Remote ID identifies the device that is inserting the DHCP Relay Agent Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the device's MAC address.

Use the **no** variant of this command to return the Remote ID for an interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay agent-option remote-id <remote-id>
no ip dhcp-relay agent-option remote-id
```

Parameter	Description
<remote-id>	An alphanumeric (ASCII) string, 1 to 63 characters in length. Additional characters allowed are hyphen (-), underscore (_) and hash (#). Spaces are not allowed.

Default The Remote ID is set to the device's MAC address by default.

Mode Interface Configuration for a VLAN interface.

Usage notes The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled (ip dhcp-relay agent-option), and
- DHCP Relay Agent is enabled on the device (service dhcp-relay)

Examples To set the Remote ID to myid for client DHCP packets received on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay agent-option remote-id
```

Related commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

show ip dhcp-relay

ip dhcp-relay information policy

Overview This command sets the policy for how the DHCP relay deals with packets arriving from the client that contain DHCP Relay Agent Option 82 information.

If the command **ip dhcp-relay agent-option** has not been configured, then this command has no effect at all - no alteration is made to Option 82 information in packets arriving from the client side.

However, if the command **ip dhcp-relay agent-option** has been configured, this command modifies how the DHCP relay service deals with cases where the packet arriving from the client side already contains DHCP Relay Agent Option 82 information.

This command sets the action that the DHCP relay should take when a received DHCP client request contains DHCP Relay Agent Option 82 information.

By default, the DHCP Relay Agent replaces any existing DHCP Relay Agent Option 82 field with its own DHCP Relay Agent field. This is equivalent to the functionality of the **replace** parameter.

The **no** variant of this command returns the policy to the default behavior - i.e. replacing the existing DHCP Relay Agent Option 82 field.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

NOTE: *The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands ip dhcp-relay agent-option and ip dhcp-relay information policy have been configured.*

Syntax

```
ip dhcp-relay information policy {append|drop|keep|replace}
no ip dhcp-relay information policy
```

Parameter	Description
`append`	The DHCP Relay Agent appends the DHCP Relay Agent Option 82 field of the packet with its own DHCP Relay Agent Option 82 details.
`drop`	The DHCP Relay Agent discards the packet.
`keep`	The DHCP Relay Agent forwards the packet without altering the DHCP Relay Agent Option 82 field.
`replace`	The DHCP Relay Agent replaces the existing DHCP Relay Agent details in the DHCP Relay Agent Option 82 field with its own details before forwarding the packet.

Mode Interface Configuration for a VLAN interface.

Examples

To make the DHCP Relay Agent listening on vlan2 drop any client requests that already contain DHCP Relay Agent Option 82 information, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay information policy drop
```

To reset the DHCP relay information policy to the default policy for interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay information policy
```

Related commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

service dhcp-server

ip dhcp-relay maxhops

Overview This command sets the hop count threshold for discarding BOOTP messages. When the hops field in a BOOTP message exceeds the threshold, the DHCP Relay Agent discards the BOOTP message. The hop count threshold is set to 10 hops by default.

Use the **no** variant of this command to reset the hop count to the default.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay maxhops <1-255>
no ip dhcp-relay maxhops
```

Parameter	Description
<1-255>	The maximum hop count value.

Default The default hop count threshold is 10 hops.

Mode Interface Configuration for a VLAN interface.

Example To set the maximum number of hops to 5 for packets received on interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay maxhops 5
```

Related commands service dhcp-relay

ip dhcp-relay max-message-length

Overview This command applies when the device is acting as a DHCP Relay Agent and DHCP Relay Agent Option 82 insertion is enabled. It sets the maximum DHCP message length (in bytes) for the DHCP packet with its DHCP Relay Agent Option 82 data inserted. From this value it calculates the maximum packet size that it will accept at its input. Packets that arrive greater than this value will be dropped.

The **no** variant of this command sets the maximum message length to its default of 1400 bytes.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay max-message-length <548-1472>
no ip dhcp-relay max-message-length
```

Parameter	Description
<548-1472>	The maximum DHCP message length (this is the message header plus the inserted DHCP option fields in bytes).

Default The default is 1400 bytes.

Mode Interface Configuration for a VLAN interface.

Usage notes When a DHCP Relay Agent (that has DHCP Relay Agent Option 82 insertion enabled) receives a request packet from a DHCP client, it will append the DHCP Relay Agent Option 82 component data, and forward the packet to the DHCP server. The DHCP client will sometimes issue packets containing pad option fields that can be overwritten with Option 82 data.

Where there are insufficient pad option fields to contain all the DHCP Relay Agent Option 82 data, the DHCP Relay Agent will increase the packet size to accommodate the DHCP Relay Agent Option 82 data. If the new (increased) packet size exceeds that defined by the **maximum-message-length** parameter, then the DHCP Relay Agent will drop the packet.

NOTE: *Before setting this command, you must first run the ip dhcp-relay agent-option command. This will allow the DHCP Relay Agent Option 82 fields to be appended.*

Example To set the maximum DHCP message length to 1200 bytes for packets arriving in interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay max-message-length 1200
```

To reset the maximum DHCP message length to the default of 1400 bytes for packets arriving in interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay max-message-length
```

Related commands service dhcp-relay

ip dhcp-relay server-address

Overview This command adds a DHCP server for the DHCP Relay Agent to forward client DHCP packets to on a particular interface. You can add up to five DHCP servers on each device interface that the DHCP Relay Agent is listening on.

The **no** variant of this command deletes the specified DHCP server from the list of servers available to the DHCP relay agent.

The **no ip dhcp-relay** command removes all DHCP relay settings from the interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}
no ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}
no ip dhcp-relay
```

Parameter	Description
<ipv4-address>	Specify the IPv4 address of the DHCP server for the DHCP Relay Agent to forward client DHCP packets to, in dotted decimal notation. The IPv4 address uses the format A.B.C.D.
<ipv6-address>	Specify the IPv6 address of the DHCPv6 server for the DHCPv6 Relay Agent to forward client DHCP packets to, in hexadecimal notation.
<server-interface>	Specify the interface name of the DHCPv6 server. It is only required for a DHCPv6 server with an IPv6 address.

Mode Interface Configuration for a VLAN interface.

Usage notes For a DHCP server with an IPv6 address you must specify the interface for the DHCP server. See examples below for configuration differences between IPv4 and IPv6 DHCP relay servers.

See also the service dhcp-relay command to enable the DHCP Relay Agent on your device. The ip dhcp-relay server-address command defines a relay destination on an interface on the device, needed by the DHCP Relay Agent to relay DHCP client packets to a DHCP server.

Examples

To enable the DHCP Relay Agent to relay DHCP packets on interface vlan2 to the DHCP server with the IPv4 address 192.0.2.200, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay server-address 192.0.2.200
```

To remove the DHCP server with the IPv4 address 192.0.2.200 from the list of servers available to the DHCP Relay Agent on interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay server-address 192.0.2.200
```

To enable the DHCP Relay Agent on your device to relay DHCP packets on interface vlan10 to the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface vlan20, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface vlan10
awplus(config-if)# ip dhcp-relay server-address
2001:0db8:010d::1 vlan20
```

To remove the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface vlan20 from the list of servers available to the DHCP Relay Agent on interface vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip dhcp-relay server-address
2001:0db8:010d::1 vlan20
```

To disable DHCP relay on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay
```

Related commands

service dhcp-relay

ip dhcp-relay use-client-side-address

Overview Use this command to configure DHCP-Relay to use the client-side interface (that is the interface receiving the DHCP client packets) IP address as the source address of the relayed DHCP packets.

Use the **no** variant of this command to disable the use of the client-side interface IP address as the source IP address for relayed DHCP packets.

Syntax

```
ip dhcp-relay use-client-side-address
no ip dhcp-relay use-client-side-address
```

Parameter	Description
`use-client-side-address`	Use the client side interface IP address as the source IP address for relayed DHCP packets.

Default By default, the server-side interface IP address is used as the source IP address of DHCP relayed packets.

Mode Global Configuration

Usage notes In most cases, there are filters placed between the DHCP relay and DHCP server which only allow DHCP packets from the client subnet to the server and back. This command allows you to configure the DHCP relay so that the relay will use the IP address of the interface **receiving** clients DHCP requests to be used as the source IP address of the relayed DHCP packets.

Example To configure the client-side IP address as the source IP address of DHCP relayed packets, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp-relay use-client-side-address
```

Output Figure 57-1: Example output from **show ip dhcp-relay**

Note that the second line of the display output shows the status of the client-side address being enabled as the source IP address.

```
awplus#sh ip dhcp-relay

DHCP Relay Service is enabled
Use of client side address as source address is enabled

vlan2 is down, line protocol is down
Maximum hop count is 10
Maximum DHCP message length is 1400
Insertion of Relay Agent Option is disabled
Checking of Relay Agent Option is disabled
Insertion of Subscriber-ID auto-MAC is disabled
The Remote Id string for Relay Agent Option is 0000.0000.0000
Relay Information policy is to replace existing relay agent information
List of servers :   10.1.1.100
```

Related commands ip dhcp-relay server-address

Command changes Version 5.4.9-0.7: command added

lease

Overview This command sets the expiration time for a leased address for the DHCP address pool you are configuring. The time set by the days, hours, minutes and seconds is cumulative. The minimum total lease time that can be configured is 20 seconds. The maximum total lease time that can be configured is 120 days.

Note that if you add a user-defined option 51 using the option command, then you will override any settings created with this command. Option 51 specifies a lease time of 1 day.

Use the **infinite** parameter to set the lease expiry time to infinite (leases never expire).

Use the **no** variant of this command to return the lease expiration time back to the default of one day.

Syntax

```
lease <days> <hours> <minutes> [<seconds>]
lease infinite
no lease
```

Parameter	Description
<days>	The number of days, from 0 to 120, that the lease expiry time is configured for. Default: 1
<hours>	The number of hours, from 0 to 24, that the lease expiry time is configured for. Default: 0
<minutes>	The number of minutes, from 0 to 60, the lease expiry time is configured for. Default: 0
<seconds>	The number of seconds, from 0 to 60, the lease expiry time is configured for.
`infinite`	The lease never expires.

Default The default lease time is 1 day.

Mode DHCP Configuration

Examples To set the lease expiration time for address pool `P2` to 35 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# lease 0 0 35
```

To set the lease expiration time for the address pool `Nerv_Office` to 1 day, 5 hours, and 30 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# lease 1 5 30
```

To set the lease expiration time for the address pool `P3` to 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P3
awplus(dhcp-config)# lease 0 0 0 20
```

To set the lease expiration time for the pool to never expire, use the command:

```
awplus(dhcp-config)# lease infinite
```

To return the lease expiration time to the default of one day, use the command:

```
awplus(dhcp-config)# no lease
```

Related commands

option

service dhcp-server

short-lease-threshold

network (DHCP)

Overview This command sets the network (subnet) that the DHCP address pool applies to.

The **no** variant of this command removes the network (subnet) from the DHCP address pool.

Syntax

```
network
{<ip-subnet-address/prefix-length>|<ip-subnet-address/mask>}
no network
```

Parameter	Description
<ip-subnet-address/prefix-length>	The IPv4 subnet address in dotted decimal notation followed by the prefix length in slash notation.
<ip-subnet-address/mask>	The IPv4 subnet address in dotted decimal notation followed by the subnet mask in dotted decimal notation.

Mode DHCP Configuration

Usage notes This command will fail if it would make existing ranges invalid. For example, if they do not lie within the new network you are configuring.

The **no** variant of this command will fail if ranges still exist in the pool. You must remove all ranges in the pool before issuing a **no network** command to remove a network from the pool.

Examples To configure a network for the address pool `P2`, where the subnet is `192.0.2.5` and the mask is `255.255.255.0`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# network 192.0.2.5/24
```

or you can use dotted decimal notation instead of slash notation for the subnet-mask:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# network 192.0.2.5 255.255.255.0
```

Related commands service dhcp-server

subnet-mask

next-server

Overview This command sets the next server address for a DHCP server pool. It is the address of the next server that the client should use in its bootstrap process.

The **no** variant of this command removes the next server address from the DHCP address pool.

Syntax

```
next-server <ip-address>
no next-server
```

Parameter	Description
<ip-address>	The server IP address, entered in dotted decimal notation.

Mode DHCP Configuration

Example To set the next-server address for the address pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# next-server 192.0.2.2
```

option

Overview This command adds a user-defined option to the DHCP address pool you are configuring. For the **hex**, **integer**, and **flag** option types, if the option already exists, the new option overwrites the existing option's value. Options with an **ip** type can hold a list of IP addresses or masks (i.e. entries that have the A.B.C.D address format), so if the option already exists in the pool, then the new IP address is added to the list of existing IP addresses.

Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

The **no** variant of this command removes the specified user-defined option from the DHCP pool, or all user-defined options from the DHCP pool.

Syntax

```
option [<1-254>|<option-name>] <option-value>
no option [<1-254>|<option-value>]
```

Parameter	Description	
<1-254>	The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.	
<option-name>	Option name associated with the option.	
<option-value>	The option value. You must specify a value that is appropriate to the option type:	
	`hex`	A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.
	`ip`	An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually using the option command multiple times.
	`integer`	A number from 0 to 4294967295.
	`flag`	A value of either true, on, or enabled to set the flag, or false, off or disabled to unset the flag.

Mode DHCP Configuration

Examples

To add the ASCII-type option named `tftp-server-name` to the pool `P2` and give the option the value `server1`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# option tftp-server-name server1
```

To add the hex-type option named `tcpip-node-type` to the pool `P2` and give the option the value `08af`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# option tcpip-node-type 08af
```

To add multiple IP addresses for the ip-type option `175`, use the command:

```
awplus(dhcp-config)# option 175 192.0.2.6
awplus(dhcp-config)# option 175 192.0.2.12
awplus(dhcp-config)# option 175 192.0.2.33
```

To add the option `179` to a pool, and give the option the value `123456`, use the command:

```
awplus(dhcp-config)# option 179 123456
```

To add a user-defined flag option with the name `perform-router-discovery`, use the command:

```
awplus(dhcp-config)# option perform-router-discovery yes
```

To clear all user-defined options from a DHCP address pool, use the command:

```
awplus(dhcp-config)# no option
```

To clear a user-defined option, named `tftp-server-name`, use the command:

```
awplus(dhcp-config)# no option tftp-server-name
```

Related commands

dns-server

ip dhcp option

lease

service dhcp-server

show ip dhcp pool

probe enable

Overview Use this command to enable lease probing for a DHCP pool. Probing is used by the DHCP server to check if an IP address it wants to lease to a client is already being used by another host.

The **no** variant of this command disables probing for a DHCP pool.

Syntax

```
probe enable
no probe enable
```

Default Probing is enabled by default.

Mode DHCP Pool Configuration

Examples To enable probing for pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe enable
```

To disable probing for pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe enable
```

Related commands

ip dhcp pool

probe packets

probe timeout

probe type

show ip dhcp pool

probe packets

Overview Use this command to specify the number of packets sent for each lease probe. Lease probing is configured on a per-DHCP pool basis. When set to 0 probing is effectively disabled.

The **no** variant of this command sets the number of probe packets sent to the default of 5.

Syntax

```
probe packets <0-10>
no probe packets
```

Parameter	Description
<0-10>	The number of probe packets sent.

Default The default is 5.

Mode DHCP Pool Configuration

Examples To set the number of probe packets to 2 for pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe packets 2
```

To set the number of probe packets to the default 5 for pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe packets
```

Related commands

probe enable

probe timeout

probe type

show ip dhcp pool

probe timeout

Overview Use this command to set the timeout value in milliseconds that the server waits for a response after each probe packet is sent. Lease probing is configured on a per-DHCP pool basis.

The **no** variant of this command sets the probe timeout value to the default setting, 200 milliseconds.

Syntax

```
probe timeout <50-5000>
no probe timeout
```

Parameter	Description
<50-5000>	Timeout interval in milliseconds.

Default The default timeout interval is 200 milliseconds.

Mode DHCP Pool Configuration

Examples To set the probe timeout value to 500 milliseconds for pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe timeout 500
```

To set the probe timeout value for pool `P2` to the default, 200 milliseconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe timeout
```

Related commands

probe enable

probe packets

probe type

show ip dhcp pool

probe type

Overview Use this command to set the probe type for a DHCP pool. The probe type specifies how the DHCP server checks whether an IP address is being used by other hosts, referred to as lease probing. If **arp** is specified, the server sends an ARP request to determine if an address is in use. If **ping** is specified, the server will send an ICMP Echo Request (ping).

The **no** variant of this command sets the probe type to the default setting, ping.

Syntax

```
probe type {arp|ping}
no probe type
```

Parameter	Description
`arp`	Probe using ARP.
`ping`	Probe using ping.

Default The default probe type is ping.

Mode DHCP Pool Configuration

Examples To set the probe type to `arp` for the pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe type arp
```

To set the probe type for the pool `P2` to the default, `ping`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe type
```

Related commands

ip dhcp pool

probe enable

probe packets

probe timeout

show ip dhcp pool

range

Overview This command adds an address range to the DHCP address pool you are configuring. The DHCP server responds to client requests received from the pool's network. It assigns an IP addresses within the specified range. The IP address range must lie within the network. You can add multiple address ranges and individual IP addresses for a DHCP pool by using this command multiple times.

The **no** variant of this command removes an address range from the DHCP pool. Use the **no range all** command to remove all address ranges from the DHCP pool.

Syntax

```
range <ip-address> [<ip-address>]
no range <ip-address> [<ip-address>]
no range all
```

Parameter	Description
<ip-address>	IPv4 address range for DHCP clients, in dotted decimal notation. The first IP address is the low end of the range, the second IP address is the high end. Specify only one IP address to add an individual IP address to the address pool.

Mode DHCP Configuration

Examples To add an address range of `192.0.2.5` to `192.0.2.16` to the pool `Nerv_Office`, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# range 192.0.2.5 192.0.2.16
```

To add the individual IP address `192.0.2.2` to a pool, use the command:

```
awplus(dhcp-config)# range 192.0.2.2
```

To remove all address ranges from a pool, use the command:

```
awplus(dhcp-config)# no range all
```

Related commands

ip dhcp pool

service dhcp-server

show ip dhcp pool

route

Overview This command allows the DHCP server to provide static routes to clients.

Syntax

```
route A.B.C.D/M A.B.C.D {both|opt249|rfc3442}
```

Parameter	Description
`A.B.C.D/M`	Subnet for the route
`A.B.C.D`	Next hop for the route
`both`	opt249 and rft3442
`opt249`	Classless static route option for DHCP
`rfc3442`	Classless static route option for DHCP

Mode DHCP Configuration

Examples To distribute static routes for route `0.0.0.0/0` whose next hop is `192.16.1.1` to clients using both `opt249` and `rfc3442`, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool pubic
awplus(dhcp-config)# route 0.0.0.0/0 192.16.1.1 both
```

Related commands ip dhcp pool

service dhcp-relay

Overview This command enables the DHCP Relay Agent on the device. However, on a given IP interface, no DHCP forwarding takes place until at least one DHCP server is specified to forward/relay all clients' DHCP packets to.

The **no** variant of this command disables the DHCP Relay Agent on the device for all interfaces.

Syntax

```
service dhcp-relay
no service dhcp-relay
```

Mode Global Configuration

Usage notes A maximum number of 400 DHCP Relay Agents (one per interface) can be configured on the device. Once this limit has been reached, any further attempts to configure DHCP Relay Agents will not be successful.

Default The DHCP-relay service is enabled by default.

Examples To enable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
```

To disable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# no service dhcp-relay
```

Related commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

ip dhcp-relay information policy

ip dhcp-relay maxhops

ip dhcp-relay server-address

service dhcp-server

Overview This command enables the DHCP server on your device. The server then listens for DHCP requests on all IP interfaces. It will not run if there are no IP interfaces configured.

The **no** variant of this command disables the DHCP server.

Syntax

```
service dhcp-server
no service dhcp-server
```

Mode Global Configuration

Example To enable the DHCP server, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-server
```

Related commands

ip dhcp pool

show ip dhcp server summary

subnet-mask

short-lease-threshold

Overview Use this command to configure a short lease threshold.

Use the **no** variant of this command to return the short lease threshold to the default of one minute.

Syntax

```
short-lease-threshold <hours> <minutes>
no short-lease-threshold
```

Parameter	Description
<hours>	The number of hours, from 0 to 24.
<minutes>	The number of minutes, from 0 to 60.

Default 1 minute.

Mode DHCP Configuration

Usage notes DHCP leases need to be backed up in NVS so that when the DHCP server reboots or goes through a power cycle it won't lose all the knowledge of these leases.

Some networks have a high number of mobile devices repeatedly requesting DHCP leases every few seconds before their existing lease expires. This can happen for example, when mobile devices move in and out of a Wi-Fi zone or when Wi-Fi signal strength changes. This means the same IP address can have multiple lease entries which can take up unnecessary backup file space.

The **short-lease-threshold** command allows you to configure the threshold for a short lease, from 1 minute to 24 hours. Any lease less than the threshold is deemed to be a short lease and will NOT be backed up to NVS.

This is useful if you have:

- limited backup file space, and
- you don't need to restore leases after a device reboot or power cycle

Example To set the short lease threshold for address pool P2 to 40 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# short-lease-threshold 0 40
```

To set the short lease threshold for address pool Nerv_Office to 5 hours and 35 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# short-lease-threshold 5 35
```

To return the short lease threshold to the default of one minute, use the following commands:

```
awplus# configure terminal
awplus(config)# no short-lease-threshold
```

Related commands lease

Command changes Version 5.4.8-2.1: command added

show counter dhcp-client

Overview This command shows counters for the DHCP client on your device.

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

Syntax

```
show counter dhcp-client
```

Mode User Exec and Privileged Exec

Example To display the message counters for the DHCP client on your device, use the command:

```
awplus# show counter dhcp-client
```

Output Figure 57-2: Example output from the **show counter dhcp-client** command

```
show counter dhcp-client

DHCPDISCOVER out      ......... 10
DHCPREQUEST out       ......... 34
DHCPDECLINE out       ......... 4
DHCPRELEASE out       ......... 0
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 counter dhcp-relay

Overview This command shows counters for the DHCP Relay Agent on your device.

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

Syntax

```
show counter dhcp-relay
```

Mode User Exec and Privileged Exec

Examples To display counters for the DHCP Relay Agent on your device, use the following command:

```
awplus# show counter dhcp-relay
```

Output Figure 57-3: Example output from the **show counter dhcp-relay** command

```
awplus#show counter dhcp-relay

DHCP relay counters
Requests In               ......... 4
Replies In                ......... 4
Relayed To Server         ......... 4
Relayed To Client         ......... 4
Out To Server Failed      ......... 0
Out To Client Failed      ......... 0
Invalid hlen              ......... 0
Bogus giaddr              ......... 0
Corrupt Agent Option      ......... 0
Missing Agent Option      ......... 0
Bad Circuit ID            ......... 0
Missing Circuit ID        ......... 0
Bad Remote ID             ......... 0
Missing Remote ID         ......... 0
Option Insert Failed      ......... 0
DHCPv6 Requests In        ......... 0
DHCPv6 Replies In         ......... 0
DHCPv6 Relayed to Server ......... 0
DHCPv6 Relayed to Client ......... 0
```

Parameter	Description
Requests In	The number of DHCP Request messages received from clients.
Replies In	The number of DHCP Reply messages received from servers.
Relayed To Server	The number of DHCP Request messages relayed to servers.
Relayed To Client	The number of DHCP Reply messages relayed to clients.

Parameter	Description
`Out To Server Failed`	The number of failures when attempting to send request messages to servers. This is an internal debugging counter.
`Out To Client Failed`	The number of failures when attempting to send reply messages to clients. This is an internal debugging counter.
`Invalid hlen`	The number of incoming messages dropped due to an invalid hlen field.
`Bogus giaddr`	The number of incoming DHCP Reply messages dropped due to the bogus giaddr field.
`Corrupt Agent Option`	The number of incoming DHCP Reply messages dropped due to a corrupt relay agent information option field. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command.
`Missing Agent Option`	The number of incoming DHCP Reply messages dropped due to a missing relay agent information option field. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command.
`Bad Circuit ID`	The number of incoming DHCP Reply messages dropped due to a bad circuit ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
`Missing Circuit ID`	The number of incoming DHCP Reply messages dropped due to a missing circuit ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command

Parameter	Description
`Bad Remote ID`	The number of incoming DHCP Reply messages dropped due to a bad remote ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
`Missing Remote ID`	The number of incoming DHCP Reply messages dropped due to a missing remote ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
`Option Insert Failed`	The number of incoming DHCP Request messages dropped due to an error adding the DHCP Relay Agent information (option-82). This counter increments when: • the DHCP Relay Agent is set to drop packets with the DHCP Relay Agent Option 82 field already filled by another DHCP Relay Agent. This policy is set with the ip dhcp-relay information policy command. • there is a packet error that stops the DHCP Relay Agent from being able to append the packet with its DHCP Relay Agent Information Option (Option 82) field.
`DHCPv6 Requests In`	The number of incoming DHCPv6 Request messages.
`DHCPv6 Replies In`	The number of incoming DHCPv6 Reply messages.
`DHCPv6 Relayed to Server`	The number of DHCPv6 messages relayed to the server.
`DHCPv6 Relayed to Client`	The number of DHCPv6 messages relayed to the client.

show counter dhcp-server

Overview This command shows counters for the DHCP server on your device.

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

Syntax

```
show counter dhcp-server
```

Mode User Exec and Privileged Exec

Example To display counters for the DHCP server on your device, use the command:

```
awplus# show counter dhcp-server
```

Output Figure 57-4: Example output from the **show counter dhcp-server** command

```
DHCP server counters
DHCPDISCOVER in       ......... 20
DHCPREQUEST in        ......... 12
DHCPDECLINE in        ......... 1
DHCPRELEASE in        ......... 0
DHCPINFORM in         ......... 0
DHCPOFFER out         ......... 8
DHCPACK out           ......... 4
DHCPNAK out           ......... 0
BOOTREQUEST in        ......... 0
BOOTREPLY out         ......... 0
```

Table 2: Parameters in the output of the **show counter dhcp-server** command

Parameter	Description
DHCPDISCOVER in	The number of Discover messages received by the DHCP server.
DHCPREQUEST in	The number of Request messages received by the DHCP server.
DHCPDECLINE in	The number of Decline messages received by the DHCP server.
DHCPRELEASE in	The number of Release messages received by the DHCP server.
DHCPINFORM in	The number of Inform messages received by the DHCP server.
DHCPOFFER out	The number of Offer messages sent by the DHCP server.
DHCPACK out	The number of Acknowledgement messages sent by the DHCP server.

Table 2: Parameters in the output of the **show counter dhcp-server** command

Parameter	Description
`DHCPNAK out`	The number of Negative Acknowledgement messages sent by the DHCP server. The server sends these after receiving a request that it cannot fulfil because either there are no available IP addresses in the related address pool, or the request has come from a client that doesn't fit the network setting for an address pool.
`BOOTREQUEST in`	The number of bootp messages received by the DHCP server from bootp clients.
`BOOTREPLY out`	The number of bootp messages sent by the DHCP server to bootp clients.

Related commands

service dhcp-server

show ip dhcp binding

show ip dhcp server statistics

show ip dhcp pool

show dhcp lease

Overview This command shows details about the leases that the DHCP client has acquired from a DHCP server for interfaces on the device.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare_Plus" Feature Overview and Configuration Guide.

Syntax

```
show dhcp lease [<interface>]
```

Parameter	Description
<interface>	Interface name to display DHCP lease details for.

Mode User Exec and Privileged Exec

Example To show the current lease expiry times for all interfaces, use the command:

```
awplus# show dhcp lease
```

To show the current lease for vlan1, use the command:

```
awplus# show dhcp lease vlan1
```

Output Figure 57-5: Example output from the **show dhcp lease vlan1** command

```
Interface vlan1
-----------------------------------------------------------------
IP Address:                    192.168.22.4
Expires:                       13 Mar 2017 20:10:19
Renew:                         13 Mar 2017 18:37:06
Rebind:                        13 Mar 2017 19:49:29
Server:
Options:
  subnet-mask                  255.255.255.0
  routers                      19.18.2.100,12.16.2.17
  dhcp-lease-time              3600
  dhcp-message-type            5
  domain-name-servers          192.168.100.50,19.88.200.33
  dhcp-server-identifier       192.168.22.1
  domain-name                  alliedtelesis.com
```

Related commands ip address dhcp

show ip dhcp binding

Overview This command shows the lease bindings that the DHCP server has allocated clients.

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

Syntax

```
show ip dhcp binding [<ip-address>|<address-pool>]
```

Parameter	Description
<ip-address>	IPv4 address of a leased IP address, in dotted decimal notation. This displays the lease information for the specified IP address.
<address-pool>	Name of an address pool. This displays the lease information for all clients within the address pool.

Mode User Exec and Privileged Exec

Examples To display all leases for every client in all address pools, use the command:

```
awplus# show ip dhcp binding
```

To display the details for the leased IP address `172.16.2.16`, use the command:

```
awplus# show ip dhcp binding 172.16.2.16
```

To display the leases from the address pool `MyPool`, use the command:

```
awplus# show ip dhcp binding MyPool
```

Output Figure 57-6: Example output from the **show ip dhcp binding** command

```
Pool 30_2_network Network 172.16.2.0/24
DHCP Client Entries
IP Address      ClientId                  Type           Expiry
-------------------------------------------------------------------------------
172.16.2.100    0050.fc82.9ede            Dynamic        21 Sep 2007 19:02:58
172.16.2.101    000e.a6ae.7c14            Static         Infinite
172.16.2.102    000e.a6ae.7c4c            Static         Infinite
172.16.2.103    000e.a69a.ac91            Static         Infinite
172.16.2.104    00e0.189d.5e41            Static         Infinite
172.16.2.150    00e0.2b04.5800            Static         Infinite
172.16.2.167    4444.4400.35c3            Dynamic        21 Sep 2007 14:58:41
```

Related commands

clear ip dhcp binding

ip dhcp pool

show ip dhcp pool

show ip dhcp pool

Overview This command displays the configuration details and system usage of the DHCP address pools configured on the device.

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

Syntax

```
show ip dhcp pool [<address-pool>]
```

Parameter	Description
<address-pool>	Name of a specific address pool. This displays the configuration of the specified address pool only.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip dhcp pool
```

Output Figure 57-7: Example output from the **show ip dhcp pool** command

```
Pool p1 :
  network: 192.168.1.0/24
  address ranges:
    addr: 192.168.1.10 to 192.168.1.18
  static host addresses:
    addr: 192.168.1.12     MAC addr: 1111.2222.3333
  lease <days:hours:minutes:seconds> <1:0:0:0>
  subnet mask: 255.255.255.0 (pool's network mask)
  Probe:                        Default Values
    Status:       Enabled       [Enabled]
    Type:         ARP           [Ping]
    Packets:      2             [5]
    Timeout:      200 msecs     [200]
  Dynamic addresses:
    Total:        8
    Leased:       2
    Utilization:  25.0 %
  Static host addresses:
    Total:        1
    Leased:       1
```

Output Figure 57-8: Example output from the **show ip dhcp pool** command with IP address 192.168.1.12 assigned to a VLAN interface on the device:

```
Pool p1 :
  network: 192.168.1.0/24
  address ranges:
    addr: 192.168.1.10 to 192.168.1.18
            (interface addr 192.168.1.12 excluded)
            (static host addr 192.168.1.12 excluded)
  static host addresses:
    addr: 192.168.1.12     MAC addr: 1111.2222.3333
            (= interface addr, so excluded)
  lease <days:hours:minutes:seconds> <1:0:0:0>
  subnet mask: 255.255.255.0 (pool's network mask)
  Probe:                       Default Values
    Status:       Enabled      [Enabled]
    Type:         ARP          [Ping]
    Packets:      2            [5]
    Timeout:      200 msecs    [200]
  Dynamic addresses:
    Total:        8
    Leased:       2
    Utilization:  25.0 %
  Static host addresses:
    Total:        1
    Leased:       1
```

Output Figure 57-9: Example output from the **show ip dhcp pool** command with a host with MAC 0000.cd38.05f9 is registered as a static host by DHCP Framed IP Lease feature from AUTHD:

```
Pool p1 :
  network: 10.1.1.0/24
  address ranges:
    addr: 10.1.1.101 to 10.1.1.199
            (static host addr 10.1.1.122 excluded)
            (static host addr 10.1.1.111 excluded)
  static host addresses:
    addr: 10.1.1.122       MAC addr: 0000.1111.2222
    addr: 10.1.1.111       MAC addr: 0000.cd38.05f9
                           Netmask : 255.255.255.0
                           Gateway : 10.1.1.1
                           Lease   : 60 seconds
                           Added by AUTHD
  lease  <1:0:0:0>
  subnet mask: 255.255.255.0 (pool's network mask)
  Probe:                        Default Values
    Status:       Enabled      [Enabled]
    Type:         Ping         [Ping]
    Packets:      5            [5]
    Timeout:      200 msecs    [200]
  Dynamic addresses:
    Total:        97
    Leased:       1
    Utilization:  1.0 %
  Static host addresses:
    Total:        2
    Leased:       2
```

Table 3: Parameters in the output of the **show ip dhcp pool** command

Parameter	Description
Pool	Name of the pool.
network	Subnet and mask length of the pool.
address ranges	Individual IP addresses and address ranges configured for the pool. The DHCP server can offer clients an IP address from within the specified ranges only. Any of these addresses that match an interface address on the device, or a static host address configured in the pool, will be automatically excluded from the range, and a message to this effect will appear beneath the range entry.

Table 3: Parameters in the output of the **show ip dhcp pool** command (cont.)

Parameter	Description
static host addresses	The static host addresses configured on the pool. Each IP address is permanently assigned to the client with the matching MAC address. Any of these addresses that match an interface address on the device will be automatically excluded, and a message to this effect will appear beneath the static host entry.
lease <days:hours:minutes>	The lease duration for address allocated by this pool.
domain	The domain name sent by the pool to clients. This is the domain name that the client should use when resolving host names using DNS.
subnet mask	The subnet mask sent by the pool to clients.
Probe - Status	Whether lease probing is enabled or disabled.
Probe - Type	The lease probe type configured. Either ping or ARP.
Probe - Packets	The number of packets sent for each lease probe in the range 0 to 10.
Probe - Timeout	The timeout value in milliseconds to wait for a response after each probe packet is sent. In the range 50 to 5000.
dns servers	The DNS server addresses sent to by the pool to clients.
default-router(s)	The default router addresses sent by the pool to clients.
user-defined options	The list of user-defined options sent by the pool to clients.
Dynamic addresses- Total	The total number of IP addresses that have been configured in the pool for dynamic allocation to DHCP clients.
Dynamic addresses- Leased	The number of IP addresses in the pool that have been dynamically allocated (leased) to DHCP clients.
Dynamic addresses - Utilization	The percentage of IP addresses in the pool that are currently dynamically allocated to clients.
Static host addresses- Total	The number of static IP addresses configured in the pool for specific DHCP client hosts.
Static host addresses - Leased	The number of static IP addresses assigned to specific DHCP client hosts.

Related commands

ip dhcp pool

probe enable

probe packets

probe timeout

probe type

range

service dhcp-server

subnet-mask

show ip dhcp-relay

Overview This command shows the configuration of the DHCP Relay Agent on each interface.

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

Syntax

```
show ip dhcp-relay [interface <interface-name>]
```

Parameter	Description
<interface-name>	Name of a specific interface. This displays the DHCP configuration for the specified interface only.

Mode User Exec and Privileged Exec

Example To display the DHCP Relay Agent's configuration on the interface vlan2, use the command:

```
awplus# show ip dhcp-relay interface vlan2
```

Output Figure 57-10: Example output from the **show ip dhcp-relay** command

```
DHCP Relay Service is enabled

vlan2 is up, line protocol is up
Maximum hop count is 10
Insertion of Relay Agent Option is disabled
Checking of Relay Agent Option is disabled
The Remote Id string for Relay Agent Option is 0000.cd28.074c
Relay information policy is to append new relay agent
information
List of servers :   192.168.1.200
```

Related commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

ip dhcp-relay information policy

ip dhcp-relay maxhops

ip dhcp-relay server-address

show ip dhcp server statistics

Overview This command shows statistics related to the DHCP server.

You can display the server counters using the show counter dhcp-server command as well as with this command.

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

Syntax

```
show ip dhcp server statistics
```

Mode User Exec and Privileged Exec

Example To display the server statistics, use the command:

```
awplus# show ip dhcp server statistics
```

Output Figure 57-11: Example output from the **show ip dhcp server statistics** command

```
DHCP server counters
DHCPDISCOVER in       ......... 20
DHCPREQUEST in        ......... 12
DHCPDECLINE in        ......... 1
DHCPRELEASE in        ......... 0
DHCPINFORM in         ......... 0
DHCPOFFER out         ......... 8
DHCPACK out           ......... 4
DHCPNAK out           ......... 0
BOOTREQUEST in        ......... 0
BOOTREPLY out         ......... 0
DHCPLEASEQUERY in       ....... 0
DHCPLEASEUNKNOWN out    ....... 0
DHCPLEASEACTIVE out     ....... 0
DHCPLEASEUNASSIGNED out ....... 0
```

Table 4: Parameters in the output of the **show ip dhcp server statistics** command

Parameter	Description
DHCPDISCOVER in	The number of Discover messages received by the DHCP server.
DHCPREQUEST in	The number of Request messages received by the DHCP server.
DHCPDECLINE in	The number of Decline messages received by the DHCP server.

Table 4: Parameters in the output of the **show ip dhcp server statistics** command (cont.)

Parameter	Description
DHCPRELEASE in	The number of Release messages received by the DHCP server.
DHCPINFORM in	The number of Inform messages received by the DHCP server.
DHCPOFFER out	The number of Offer messages sent by the DHCP server.
DHCPACK out	The number of Acknowledgement messages sent by the DHCP server.
DHCPNAK out	The number of Negative Acknowledgement messages sent by the DHCP server. The server sends these after receiving a request that it cannot fulfil because either there are no available IP addresses in the related address pool, or the request has come from a client that doesn't fit the network setting for an address pool.
BOOTREQUEST in	The number of bootp messages received by the DHCP server from bootp clients.
BOOTREPLY out	The number of bootp messages sent by the DHCP server to bootp clients.
DHCPLEASEQUERY in	The number of Lease Query messages received by the DHCP server from DHCP Relay Agents.
DHCPLEASEUNKNOWN out	The number of Lease Unknown messages sent by the DHCP server to DHCP Relay Agents.
DHCPLEASEACTIVE out	The number of Lease Active messages sent by the DHCP server to DHCP Relay Agents.
DHCPLEASEUNASSIGNED out	The number of Lease Unassigned messages sent by the DHCP server to DHCP Relay Agents.

Related commands

show counter dhcp-server

service dhcp-server

show ip dhcp binding

show ip dhcp pool

show ip dhcp server summary

Overview This command shows the current configuration of the DHCP server. This includes:

- whether the DHCP server is enabled
- whether the DHCP server is configured to ignore BOOTP requests
- whether the DHCP server is configured to support DHCP lease queries
- the details of any user-defined options
- a list of the names of all DHCP address pools currently configured

This show command does not include any configuration details of the address pools. You can display these using the show ip dhcp pool command.

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

Syntax

```
show ip dhcp server summary
```

Mode User Exec and Privileged Exec

Example To display the current configuration of the DHCP server, use the command:

```
awplus# show ip dhcp server summary
```

Output Figure 57-12: Example output from the **show ip dhcp server summary** command

```
DHCP Server service is disabled
BOOTP ignore is disabled
DHCP leasequery support is disabled
Pool list: p2
```

Related commands

ip dhcp leasequery enable

ip dhcp pool

service dhcp-server

subnet-mask

Overview This command sets the subnet mask option for a DHCP address pool you are configuring. Use this command to specify the client's subnet mask as defined in RFC 950. This sets the subnet details using the pre-defined option 1. Note that if you create a user-defined option 1 using the option command, then you will override any settings created with this command. If you do not specify a subnet mask using this command, then the pool's network mask (specified using the next-server command) is applied.

The **no** variant of this command removes a subnet mask option from a DHCP pool. The pool reverts to using the pool's network mask.

Syntax

```
subnet-mask <mask>
no subnet-mask
```

Parameter	Description
<mask>	Valid IPv4 subnet mask, in dotted decimal notation.

Mode DHCP Configuration

Examples To set the subnet mask option to `255.255.255.0` for DHCP pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# subnet-mask 255.255.255.0
```

To remove the subnet mask option from DHCP pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no subnet-mask
```

Related commands

default-router

dns-server

domain-name

show ip dhcp pool

58 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 2995
- "clear ipv6 dhcp client" on page 2996
- "ip dhcp-relay agent-option" on page 2997
- "ip dhcp-relay agent-option subscriber-id-auto-mac" on page 2999
- "ip dhcp-relay agent-option checking" on page 3000
- "ip dhcp-relay agent-option remote-id" on page 3001
- "ip dhcp-relay information policy" on page 3002
- "ip dhcp-relay maxhops" on page 3004
- "ip dhcp-relay max-message-length" on page 3005
- "ip dhcp-relay server-address" on page 3007
- "ipv6 address dhcp" on page 3009

- "service dhcp-relay" on page 3011
- "show counter dhcp-relay" on page 3012
- "show counter ipv6 dhcp-client" on page 3015
- "show ip dhcp-relay" on page 3017
- "show ipv6 dhcp" on page 3018
- "show ipv6 dhcp interface" on page 3019

clear counter ipv6 dhcp-client

Overview Use this command in Privileged Exec mode to clear DHCPv6 client counters.

Syntax

```
clear counter ipv6 dhcp-client
```

Mode Privileged Exec

Example To clear DHCPv6 client counters, use the following command:

```
awplus# clear counter ipv6 dhcp-client
```

Related commands show counter ipv6 dhcp-client

clear ipv6 dhcp client

Overview Use this command in Privileged Exec mode to restart a DHCPv6 client on an interface.

Syntax `clear ipv6 dhcp client <interface>`

Parameter	Description
<interface>	Specify the interface name to restart a DHCPv6 client on.

Mode Privileged Exec

Example To restart a DHCPv6 client on interface vlan1, use the following command:

```
awplus# clear ipv6 dhcp client vlan1
```

ip dhcp-relay agent-option

Overview This command enables the DHCP Relay Agent to insert the DHCP Relay Agent Information Option (Option 82) into the client-request packets that it relays to its DHCP server. This allows the DHCP Relay Agent to pass on information to the server about the network location of the client device. The DHCP Relay Agent strips the DHCP Relay Agent Option 82 field out of the DHCP server's response, so that the DHCP client never sees this field.

When the DHCP Relay Agent appends its DHCP Relay Agent Option 82 data into the packet, it first overwrites any pad options present; then if necessary, it increases the packet length to accommodate the DHCP Relay Agent Option 82 data.

The **no** variant of this command stops the DHCP Relay Agent from appending the Option 82 field onto DHCP requests before forwarding it to the server.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

NOTE: *The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands ip dhcp-relay agent-option and ip dhcp-relay information policy have been configured.*

Syntax

```
ip dhcp-relay agent-option
no ip dhcp-relay agent-option
```

Default DHCP Relay Agent Information Option (Option 82) insertion is disabled by default.

Mode Interface Configuration for a VLAN interface.

Usage notes Use this command to alter the DHCP Relay Agent Option 82 setting when your device is the first hop for the DHCP client. To limit the maximum length of the packet, use the ip dhcp-relay max-message-length command.

This command cannot be enabled if DHCP snooping is enabled on your device (service dhcp-snooping command), and vice versa.

Examples To make the DHCP Relay Agent listening on vlan2 append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the DHCP Relay Agent from appending the DHCP Relay Agent Option 82 field on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay agent-option
```

Related commands

ip dhcp-relay agent-option remote-id

ip dhcp-relay information policy

ip dhcp-relay max-message-length

service dhcp-relay

ip dhcp-relay agent-option subscriber-id-auto-mac

Overview This command causes the relay agent to insert the requesting clients' MAC address into a subscriber ID field in the relay header. A suitably-configured server can then use this subscriber ID option to assign the same IPv6 address to that requesting client every time it requires an address.

Use the no form of this command to disable this feature.

Syntax

```
ip dhcp-relay agent-option subscriber-id-auto-mac
no ip dhcp-relay agent-option subscriber-id-auto-mac
```

Default Disabled

Usage notes By default, DHCPv6 uses a DUID-LLT client identifier instead of a MAC address. This is generated by the operating system when DHCP first starts. If the OS is reinstalled the DUID-LLT can change, and any multiple operating systems on the machine will all have different DUIDs.

Configuring the subscriber-id-auto-mac option causes the relay agent to insert the requesting client's MAC address into a subscriber ID field in the relay header. A suitably-configured server can then use this subscriber ID to assign the same IPv6 address to that requesting client every time it connects.

The client must be in the same L2 network as the relay. If there are multiple relays between the client and the server, only the first relay will add a subscriber ID option.

Example To enable this feature on VLAN1, use the following commands:

```
awplus(config)#int vlan1
awplus(config-if)#ip dhcp-relay agent-option
subscriber-id-auto-mac
```

For an example of how to configure a relay agent and server, see the document "How to use DHCPv6 to assign specific IPv6 addresses to specific devices", available from www.alliedtelesis.com.

ip dhcp-relay agent-option checking

Overview This command enables the DHCP Relay Agent to check DHCP Relay Agent Information Option (Option 82) information in response packets returned from DHCP servers. If the information does not match the information it has for its own client (downstream) interface then the DHCP Relay Agent drops the packet. Note that ip dhcp-relay agent-option must be configured.

The DHCP Relay Agent Option 82 field is included in relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled (ip dhcp-relay agent-option), and
- DHCP Relay Agent is enabled on the device (service dhcp-relay)

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay agent-option checking
no ip dhcp-relay agent-option checking
```

Mode Interface Configuration for a VLAN interface.

Examples To make the DHCP Relay Agent listening on vlan2 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay agent-option
awplus(config-if)# ip dhcp-relay agent-option checking
```

To stop the DHCP Relay Agent on vlan2 from checking the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay agent-option checking
```

Related commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option remote-id

ip dhcp-relay information policy

service dhcp-relay

ip dhcp-relay agent-option remote-id

Overview Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field the DHCP Relay Agent inserts into clients' request packets. The Remote ID identifies the device that is inserting the DHCP Relay Agent Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the device's MAC address.

Use the **no** variant of this command to return the Remote ID for an interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay agent-option remote-id <remote-id>
no ip dhcp-relay agent-option remote-id
```

Parameter	Description
<remote-id>	An alphanumeric (ASCII) string, 1 to 63 characters in length. Additional characters allowed are hyphen (-), underscore (_) and hash (#). Spaces are not allowed.

Default The Remote ID is set to the device's MAC address by default.

Mode Interface Configuration for a VLAN interface.

Usage notes The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled (ip dhcp-relay agent-option), and
- DHCP Relay Agent is enabled on the device (service dhcp-relay)

Examples To set the Remote ID to myid for client DHCP packets received on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay agent-option remote-id
```

Related commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

show ip dhcp-relay

ip dhcp-relay information policy

Overview This command sets the policy for how the DHCP relay deals with packets arriving from the client that contain DHCP Relay Agent Option 82 information.

If the command **ip dhcp-relay agent-option** has not been configured, then this command has no effect at all - no alteration is made to Option 82 information in packets arriving from the client side.

However, if the command **ip dhcp-relay agent-option** has been configured, this command modifies how the DHCP relay service deals with cases where the packet arriving from the client side already contains DHCP Relay Agent Option 82 information.

This command sets the action that the DHCP relay should take when a received DHCP client request contains DHCP Relay Agent Option 82 information.

By default, the DHCP Relay Agent replaces any existing DHCP Relay Agent Option 82 field with its own DHCP Relay Agent field. This is equivalent to the functionality of the **replace** parameter.

The **no** variant of this command returns the policy to the default behavior - i.e. replacing the existing DHCP Relay Agent Option 82 field.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

NOTE: *The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands ip dhcp-relay agent-option and ip dhcp-relay information policy have been configured.*

Syntax

```
ip dhcp-relay information policy {append|drop|keep|replace}
no ip dhcp-relay information policy
```

Parameter	Description
`append`	The DHCP Relay Agent appends the DHCP Relay Agent Option 82 field of the packet with its own DHCP Relay Agent Option 82 details.
`drop`	The DHCP Relay Agent discards the packet.
`keep`	The DHCP Relay Agent forwards the packet without altering the DHCP Relay Agent Option 82 field.
`replace`	The DHCP Relay Agent replaces the existing DHCP Relay Agent details in the DHCP Relay Agent Option 82 field with its own details before forwarding the packet.

Mode Interface Configuration for a VLAN interface.

Examples

To make the DHCP Relay Agent listening on vlan2 drop any client requests that already contain DHCP Relay Agent Option 82 information, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay information policy drop
```

To reset the DHCP relay information policy to the default policy for interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay information policy
```

Related commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

service dhcp-server

ip dhcp-relay maxhops

Overview This command sets the hop count threshold for discarding BOOTP messages. When the hops field in a BOOTP message exceeds the threshold, the DHCP Relay Agent discards the BOOTP message. The hop count threshold is set to 10 hops by default.

Use the **no** variant of this command to reset the hop count to the default.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay maxhops <1-255>
no ip dhcp-relay maxhops
```

Parameter	Description
<1-255>	The maximum hop count value.

Default The default hop count threshold is 10 hops.

Mode Interface Configuration for a VLAN interface.

Example To set the maximum number of hops to 5 for packets received on interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay maxhops 5
```

Related commands service dhcp-relay

ip dhcp-relay max-message-length

Overview This command applies when the device is acting as a DHCP Relay Agent and DHCP Relay Agent Option 82 insertion is enabled. It sets the maximum DHCP message length (in bytes) for the DHCP packet with its DHCP Relay Agent Option 82 data inserted. From this value it calculates the maximum packet size that it will accept at its input. Packets that arrive greater than this value will be dropped.

The **no** variant of this command sets the maximum message length to its default of 1400 bytes.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay max-message-length <548-1472>
no ip dhcp-relay max-message-length
```

Parameter	Description
<548-1472>	The maximum DHCP message length (this is the message header plus the inserted DHCP option fields in bytes).

Default The default is 1400 bytes.

Mode Interface Configuration for a VLAN interface.

Usage notes When a DHCP Relay Agent (that has DHCP Relay Agent Option 82 insertion enabled) receives a request packet from a DHCP client, it will append the DHCP Relay Agent Option 82 component data, and forward the packet to the DHCP server. The DHCP client will sometimes issue packets containing pad option fields that can be overwritten with Option 82 data.

Where there are insufficient pad option fields to contain all the DHCP Relay Agent Option 82 data, the DHCP Relay Agent will increase the packet size to accommodate the DHCP Relay Agent Option 82 data. If the new (increased) packet size exceeds that defined by the **maximum-message-length** parameter, then the DHCP Relay Agent will drop the packet.

NOTE: *Before setting this command, you must first run the ip dhcp-relay agent-option command. This will allow the DHCP Relay Agent Option 82 fields to be appended.*

Example To set the maximum DHCP message length to 1200 bytes for packets arriving in interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay max-message-length 1200
```

To reset the maximum DHCP message length to the default of 1400 bytes for packets arriving in interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay max-message-length
```

Related commands service dhcp-relay

ip dhcp-relay server-address

Overview This command adds a DHCP server for the DHCP Relay Agent to forward client DHCP packets to on a particular interface. You can add up to five DHCP servers on each device interface that the DHCP Relay Agent is listening on.

The **no** variant of this command deletes the specified DHCP server from the list of servers available to the DHCP relay agent.

The **no ip dhcp-relay** command removes all DHCP relay settings from the interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}
```

```
no ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}
```

```
no ip dhcp-relay
```

Parameter	Description
<ipv4-address>	Specify the IPv4 address of the DHCP server for the DHCP Relay Agent to forward client DHCP packets to, in dotted decimal notation. The IPv4 address uses the format A.B.C.D.
<ipv6-address>	Specify the IPv6 address of the DHCPv6 server for the DHCPv6 Relay Agent to forward client DHCP packets to, in hexadecimal notation.
<server-interface>	Specify the interface name of the DHCPv6 server. It is only required for a DHCPv6 server with an IPv6 address.

Mode Interface Configuration for a VLAN interface.

Usage notes For a DHCP server with an IPv6 address you must specify the interface for the DHCP server. See examples below for configuration differences between IPv4 and IPv6 DHCP relay servers.

See also the service dhcp-relay command to enable the DHCP Relay Agent on your device. The ip dhcp-relay server-address command defines a relay destination on an interface on the device, needed by the DHCP Relay Agent to relay DHCP client packets to a DHCP server.

Examples

To enable the DHCP Relay Agent to relay DHCP packets on interface vlan2 to the DHCP server with the IPv4 address 192.0.2.200, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay server-address 192.0.2.200
```

To remove the DHCP server with the IPv4 address 192.0.2.200 from the list of servers available to the DHCP Relay Agent on interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay server-address 192.0.2.200
```

To enable the DHCP Relay Agent on your device to relay DHCP packets on interface vlan10 to the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface vlan20, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface vlan10
awplus(config-if)# ip dhcp-relay server-address
2001:0db8:010d::1 vlan20
```

To remove the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface vlan20 from the list of servers available to the DHCP Relay Agent on interface vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip dhcp-relay server-address
2001:0db8:010d::1 vlan20
```

To disable DHCP relay on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay
```

Related commands

service dhcp-relay

ipv6 address dhcp

Overview Use this command to activate the DHCPv6 client on the interface that you are configuring. This allows the interface to use the DHCPv6 client to obtain its IPv6 configuration details from a DHCPv6 server on its connected network.

The command also enables IPv6 on the interface, which creates an EUI-64 link-local address as well as enabling RA processing and SLAAC.

Use the **no** variant of this command to stop the interface from obtaining IPv6 configuration details from a DHCPv6 server.

The DHCPv6 client supports the following IP configuration options:

- Option 1—the subnet mask for your device.
- Option 3—a list of default routers.
- Option 6— list of DNS servers.
- Option 15—a domain name used to resolve host names.
- 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 a VLAN interface or a local loopback interface.

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 vlan2 to use DHCPv6 to obtain an IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 address dhcp
```

To stop the interface vlan2 from using DHCPv6 to obtain its IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address dhcp
```

Related commands

clear ipv6 dhcp client

ipv6 address

show ipv6 dhcp interface

show running-config

service dhcp-relay

Overview This command enables the DHCP Relay Agent on the device. However, on a given IP interface, no DHCP forwarding takes place until at least one DHCP server is specified to forward/relay all clients' DHCP packets to.

The **no** variant of this command disables the DHCP Relay Agent on the device for all interfaces.

Syntax

```
service dhcp-relay
no service dhcp-relay
```

Mode Global Configuration

Usage notes A maximum number of 400 DHCP Relay Agents (one per interface) can be configured on the device. Once this limit has been reached, any further attempts to configure DHCP Relay Agents will not be successful.

Default The DHCP-relay service is enabled by default.

Examples To enable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
```

To disable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# no service dhcp-relay
```

Related commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

ip dhcp-relay information policy

ip dhcp-relay maxhops

ip dhcp-relay server-address

show counter dhcp-relay

Overview This command shows counters for the DHCP Relay Agent on your device.

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

Syntax

```
show counter dhcp-relay
```

Mode User Exec and Privileged Exec

Examples To display counters for the DHCP Relay Agent on your device, use the following command:

```
awplus# show counter dhcp-relay
```

Output Figure 58-1: Example output from the **show counter dhcp-relay** command

```
awplus#show counter dhcp-relay

DHCP relay counters
Requests In               ......... 4
Replies In                ......... 4
Relayed To Server         ......... 4
Relayed To Client         ......... 4
Out To Server Failed      ......... 0
Out To Client Failed      ......... 0
Invalid hlen              ......... 0
Bogus giaddr              ......... 0
Corrupt Agent Option      ......... 0
Missing Agent Option      ......... 0
Bad Circuit ID            ......... 0
Missing Circuit ID        ......... 0
Bad Remote ID             ......... 0
Missing Remote ID         ......... 0
Option Insert Failed      ......... 0
DHCPv6 Requests In        ......... 0
DHCPv6 Replies In         ......... 0
DHCPv6 Relayed to Server ......... 0
DHCPv6 Relayed to Client ......... 0
```

Parameter	Description
Requests In	The number of DHCP Request messages received from clients.
Replies In	The number of DHCP Reply messages received from servers.
Relayed To Server	The number of DHCP Request messages relayed to servers.
Relayed To Client	The number of DHCP Reply messages relayed to clients.

Parameter	Description
`Out To Server Failed`	The number of failures when attempting to send request messages to servers. This is an internal debugging counter.
`Out To Client Failed`	The number of failures when attempting to send reply messages to clients. This is an internal debugging counter.
`Invalid hlen`	The number of incoming messages dropped due to an invalid hlen field.
`Bogus giaddr`	The number of incoming DHCP Reply messages dropped due to the bogus giaddr field.
`Corrupt Agent Option`	The number of incoming DHCP Reply messages dropped due to a corrupt relay agent information option field. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command.
`Missing Agent Option`	The number of incoming DHCP Reply messages dropped due to a missing relay agent information option field. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command.
`Bad Circuit ID`	The number of incoming DHCP Reply messages dropped due to a bad circuit ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
`Missing Circuit ID`	The number of incoming DHCP Reply messages dropped due to a missing circuit ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command

Parameter	Description
`Bad Remote ID`	The number of incoming DHCP Reply messages dropped due to a bad remote ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
`Missing Remote ID`	The number of incoming DHCP Reply messages dropped due to a missing remote ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
`Option Insert Failed`	The number of incoming DHCP Request messages dropped due to an error adding the DHCP Relay Agent information (option-82). This counter increments when: • the DHCP Relay Agent is set to drop packets with the DHCP Relay Agent Option 82 field already filled by another DHCP Relay Agent. This policy is set with the ip dhcp-relay information policy command. • there is a packet error that stops the DHCP Relay Agent from being able to append the packet with its DHCP Relay Agent Information Option (Option 82) field.
`DHCPv6 Requests In`	The number of incoming DHCPv6 Request messages.
`DHCPv6 Replies In`	The number of incoming DHCPv6 Reply messages.
`DHCPv6 Relayed to Server`	The number of DHCPv6 messages relayed to the server.
`DHCPv6 Relayed to Client`	The number of DHCPv6 messages relayed to the client.

show counter ipv6 dhcp-client

Overview Use this command in User Exec or Privilege Exec mode to show DHCPv6 client counter information.

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 58-2: 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 ip dhcp-relay

Overview This command shows the configuration of the DHCP Relay Agent on each interface.

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

Syntax

```
show ip dhcp-relay [interface <interface-name>]
```

Parameter	Description
<interface-name>	Name of a specific interface. This displays the DHCP configuration for the specified interface only.

Mode User Exec and Privileged Exec

Example To display the DHCP Relay Agent's configuration on the interface vlan2, use the command:

```
awplus# show ip dhcp-relay interface vlan2
```

Output Figure 58-3: Example output from the **show ip dhcp-relay** command

```
DHCP Relay Service is enabled

vlan2 is up, line protocol is up
Maximum hop count is 10
Insertion of Relay Agent Option is disabled
Checking of Relay Agent Option is disabled
The Remote Id string for Relay Agent Option is 0000.cd28.074c
Relay information policy is to append new relay agent
information
List of servers :   192.168.1.200
```

Related commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

ip dhcp-relay information policy

ip dhcp-relay maxhops

ip dhcp-relay server-address

show ipv6 dhcp

Overview Use this command in User Exec or Privileged Exec mode to show the DHCPv6 unique identifier (DUID) configured on your device.

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

Syntax

```
show ipv6 dhcp
```

Mode User Exec and Privileged Exec

Usage notes The DUID is based on the link-layer address for both DHCPv6 client and DHCPv6 server identifiers. The device uses the MAC address from the lowest interface number for the DUID.

The DUID is used by a DHCPv6 client to obtain an IPv6 address from a DHCPv6 server. A DHCPv6 server compares the DUID with its database of DUIDs and sends configuration data for an IPv6 address plus the preferred and valid lease time values to a DHCPv6 client.

Example To display the DUID configured on your device, use the command:

```
awplus# show ipv6 dhcp
```

Output Figure 58-4: Example output from the **show ipv6 dhcp** command

```
awplus#show ipv6 dhcp
DHCPv6 Server DUID: 0001000117ab6876001577f7ba23
```

Related commands ipv6 address dhcp

show ipv6 dhcp interface

Overview Use this command in User Exec or Privileged Exec mode to display DHCPv6 information for a specified interface, or all interfaces when entered without the interface parameter.

For information on filtering and saving command output, see 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 58-5: Example output from the **show ipv6 dhcp interface** command

```
awplus# show ipv6 dhcp interface
vlan1 is in client mode
 Address 1001::3c0:1
         preferred lifetime 9000, valid lifetime 5000
         starts  at 20 Jan 2012 09:21:35
         expires at 20 Jan 2012 10:25:32
```

Table 2: Parameters in the output of the **show counter dhcp-client** command

Parameter	Description
`<interface> is in client mode`	Displays that the specified interface is in client mode.
`Address`	Displays the address of the DHCPv6 server on the interface.
`Preference`	Displays the preference value for the DHCPv6 server.

59 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 3021
- "ntp broadcastdelay" on page 3023
- "ntp master" on page 3024
- "ntp peer" on page 3025
- "ntp rate-limit" on page 3027
- "ntp restrict" on page 3028
- "ntp server" on page 3030
- "ntp source" on page 3032
- "show ntp associations" on page 3034
- "show ntp counters" on page 3036
- "show ntp counters associations" on page 3037
- "show ntp status" on page 3038

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]
```

When in secure mode, MD5 is not available and the syntax in config files will be:

```
ntp authentication-key <keynumber> sha1-encrypted
<encrypted-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.
sha1-encrypted	This parameter indicates in running config that the key is in its encrypted form instead of in plaintext. If secure mode is enabled and you enter a SHA1 key, the running config will display this sha1-encrypted parameter instead of sha1, and will display the key in encrypted form. Do not enter a key using the sha1-encrypted parameter. Instead, enter sha1 and the unencrypted key string.
<encrypted-key-string>	The encrypted authentication key.
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>}
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 See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv4 address of `192.0.2.23`:

```
awplus# configure terminal
awplus(config)# ntp peer 192.0.2.23
awplus(config)# ntp peer 192.0.2.23 prefer
awplus(config)# ntp peer 192.0.2.23 prefer version 4
awplus(config)# ntp peer 192.0.2.23 prefer version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4
awplus(config)# ntp peer 192.0.2.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of `192.0.2.23`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 192.0.2.23
```

See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv6 address of 2001:0db8:010d::1:

```
awplus# configure terminal
awplus(config)# ntp peer 2001:0db8:010d::1
awplus(config)# ntp peer 2001:0db8:010d::1 prefer
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4 key
1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4 key 1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4
awplus(config)# ntp peer 2001:0db8:010d::1 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of 2001:0db8:010d::1, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 2001:0db8:010d::1
```

Related commands

ntp server

ntp source

ntp 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.

Use the **no** variant of this command to remove the configured NTP server.

Syntax

```
ntp server {<serveraddress>|<servername>}
ntp server {<serveraddress>|<servername>} [prefer] [key <key>] [version <version>]
no ntp server {<serveraddress>|<servername>}
```

Parameter	Description
<serveraddress>	Specify the IP address of the peer, entered in the form `A.B.C.D` for an IPv4 address, or in the form `X:X::X.X` for an IPv6 address.
<servername>	Specify the server hostname. The server hostname can resolve to an IPv4 and an IPv6 address.
`prefer`	Prefer this server when possible.
`key <key>`	*<1-4294967295>* Configure the server authentication key.
`version <version>`	*<1-4>* Configure for this NTP version.

Mode Global Configuration

Examples See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv4 address of 192.0.1.23:

```
awplus# configure terminal
awplus(config)# ntp server 192.0.1.23
awplus(config)# ntp server 192.0.1.23 prefer
awplus(config)# ntp server 192.0.1.23 prefer version 4
awplus(config)# ntp server 192.0.1.23 prefer version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4
awplus(config)# ntp server 192.0.1.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of 192.0.1.23, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp server 192.0.1.23
```

See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv6 address of 2001:0db8:010e::2:

```
awplus# configure terminal
awplus(config)# ntp server 2001:0db8:010e::2
awplus(config)# ntp server 2001:0db8:010e::2 prefer
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4 key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4
awplus(config)# ntp server 2001:0db8:010e::2 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of 2001:0db8:010e::2, use the 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.

Note that you cannot use this command when using AMF (Allied Telesis Management Framework).

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 59-1: 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 59-2: 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 59-2: 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 59-1: 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 59-3: 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 59-2: 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 59-4: 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 59-3: 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
```

60 Precision Time Protocol (PTP) and Transparent Clock Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure Precision Time Protocol (PTP) and Transparent Clock.

For more information, see the Precision Time Protocol (PTP) and Transparent Clock Feature Overview and Configuration Guide.

Command List

- "clock-port" on page 3040
- "ptp-clk" on page 3041
- "ptp global" on page 3043
- "show ptp data transparent" on page 3044
- "show ptp port" on page 3045

clock-port

Overview Use this command to associate the port with the clock and enable the required PTP functionality for 1588v2 packets entering and leaving this port. For the transparent clock, this specifically means modification of the Correction Factor to reflect the residence time in the bridge.

Use the **no** variant of this command to remove the port from the clock and disable modification of the Correction Factor.

Syntax

```
clock-port
no clock-port
```

Default Ports are unassociated and disabled with the clock by default.

Mode Interface Configuration (port)

Example To configure the clock-port on port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# clock-port
```

To remove port1.0.1 from the clock and disable modification of the Correction Factor, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no clock-port
```

Related commands

ptp global

ptp-clk

show ptp data transparent

show ptp port

Command changes Version 5.4.7-0.1: command added

Version 5.4.8-0.2: added to x230, x550 series products

ptp-clk

Overview Use this command to configure the PTP clock instance on the switch. All values must be specified.

Use the **no** variant of this command to disable the clock and disable timing support on any other ports that were set as clock-ports.

Syntax

```
ptp-clk {ordinary|boundary|transparent} transport-type {udp {v4|v6}|ethernet} delay-mechanism {e2e|p2p} step-type {onestep|twostep}
```

```
no ptp-clk
```

Parameter	Description
`ordinary`	An ordinary clock, able to act as Master, Slave, or Grand Master
`boundary`	A clock able to manage downstream fan-out for an upstream Master
`transparent`	A device that acts as a bridge between a Master and a Slave and participates in the timing protocol by adding the bridge residence time to the correction factor in the packets
`udp v4`	Timing protocol forwarded in IPv4 UDP Packets
`udp v6`	Timing protocol forwarded in IPv6 UDP Packets
`ethernet`	Timing protocol forwarded in Ethernet frames
`e2e`	Specifies that the clock supports end to end messaging sequences between the Master and the Slave and that the Correction Factor is updated based on the Bridge residence time. A Delay_Request sequence is required to determine the link delay
`p2p`	Specifies that the clock supports end to end messaging sequences between the Master and the Slave as well as peer to peer messaging sequences to determine the link delay between this device and its peers. The Correction Factor is updated based on the Bridge residence time plus the peer to peer link delay - so there is no need for a delay_request message sequence.
`onestep`	Specifies that the clock supports modification of the correction factor as the message is transiting the switch
`twostep`	Specifies that the clock requires that a follow-up message be sent that is used to carry the correction factor for the previous 1588v2 message (sync, delay_request or pdelay_req)

Default This command is disabled by default.

Mode Global configuration

Usage notes The clock is not active until the PTP timing service is enabled via the **ptp global** command. It is not possible to make a port a clock port - if the clock has not been configured.

Example To configure a PTP instance on the switch, use the following commands:

```
awplus# configure terminal
awplus(config)# ptp-clk transparent transport-type ethernet
delay-mechanism e2e step-type onestep
```

Related commands ptp global

show ptp data transparent

show ptp port

Command changes Version 5.4.7- 0.1: command added

Version 5.4.8-0.2: added to x230, x550 series products

ptp global

Overview Use this command to enable 1588v2 based timing support on the device.

Use the **no** variant of this command to disable the timing support.

Syntax

```
ptp global
no ptp global
```

Default Disabled

Mode Global Configuration

Example To enable 1588v2 timing support on the switch, use the commands:

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

To disable 1588v2 timing support on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# no ptp global
```

Related commands

clock-port

ptp-clk

show ptp data transparent

show ptp port

Command changes Version 5.4.7-0.1: command added

Version 5.4.8-0.2: added to x230, x550 series products

show ptp data transparent

Overview Use this command to display configuration information for the PTP transparent clock.

Syntax

```
show ptp data transparent
```

Mode Privileged Exec

Example To display configuration for PTP transparent clock, use the following command:

```
awplus# show ptp data transparent
```

Output Figure 60-1: Example output from **show ptp data transparent**

```
IE300-1#show ptp data transparent
CLOCK(Transparent)
Global Enable          :  Enabled
Clock Identity         :  00:0c:25:ff:fe:03:92:47
Number Of Ports        :  2
Transport Type         :  Ethernet
Delay Mechanism        :  End To End
Primary Domain         :  0
Step-type              :  One Step
```

Related commands ptp-clk

Command changes Version 5.4.7-0.1: command added

Version 5.4.8-0.2: added to x230, x550 series products

show ptp port

Overview Use this command to display the configuration and status information of the individual ports that have been associated with the clock.

Syntax

```
show ptp port
```

Mode Privileged Exec

Example To display configuration and status information of the individual ports associated with the clock, use the command:

```
awplus# show ptp port
```

Output Figure 60-2: Example output from **show ptp port**

```
IE300-1#show ptp port
=================================================================
% Transparent clock
Global Enable                              :  Enabled
Clock Identity                             :
00:0c:25:ff:fe:03:92:47
Port Number                                :  1 (Interface
port1.0.1)
Peer Delay Request Interval (log base 2)   :  1
Peer Mean Path Delay                       :  0
Faulty Flag                                :  False
=================================================================
% Transparent clock
Global Enable                              :  Enabled
Clock Identity                             :
00:0c:25:ff:fe:03:92:47
Port Number                                :  2 (Interface
port1.0.2)
Peer Delay Request Interval (log base 2)   :  1
Peer Mean Path Delay                       :  0
Faulty Flag                                :  False
```

Related commands ptp-clk

Command changes Version 5.4.7-0.1: command added

Version 5.4.8-0.2: added to x230, x550 series products

61 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 3048
- "debug snmp" on page 3049
- "show counter snmp-server" on page 3050
- "show debugging snmp" on page 3054
- "show running-config snmp" on page 3055
- "show snmp-server" on page 3056
- "show snmp-server community" on page 3057
- "show snmp-server group" on page 3058
- "show snmp-server user" on page 3059
- "show snmp-server view" on page 3060
- "snmp trap link-status" on page 3061
- "snmp trap link-status suppress" on page 3062
- "snmp-server" on page 3064
- "snmp-server community" on page 3066
- "snmp-server contact" on page 3067
- "snmp-server enable trap" on page 3068

- "snmp-server engineID local" on page 3071
- "snmp-server engineID local reset" on page 3073
- "snmp-server group" on page 3074
- "snmp-server host" on page 3076
- "snmp-server legacy-ifadminstatus" on page 3078
- "snmp-server location" on page 3079
- "snmp-server source-interface" on page 3080
- "snmp-server startup-trap-delay" on page 3081
- "snmp-server user" on page 3082
- "snmp-server view" on page 3085
- "undebug snmp" on page 3086

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 port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# alias uplink_a
```

To remove an alias interface name from port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
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 61-1: 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 61-2: 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 61-3: 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 61-4: 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 61-5: 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 61-6: Example output from the **show snmp-server group** command

```
SNMP group information:
  Group name ............... guireadgroup
    Security Level ......... priv
    Read View .............. guiview
    Write View ............. none
    Notify View ............ none

  Group name ............... guiwritegroup
    Security Level ......... priv
    Read View .............. none
    Write View ............. guiview
    Notify View ............ none
```

Related commands show snmp-server

snmp-server group

show snmp-server user

Overview This command displays the SNMP server users and is used with SNMP version 3 only.

Syntax
```
show snmp-server user
```

Mode Privileged Exec

Example To display the SNMP server users configured on the device, use the command:

```
awplus# show snmp-server user
```

Output Figure 61-7: Example output from the **show snmp-server user** command

```
Name                Group name          Auth        Privacy
-------             -------------       -------     ----------
freddy              guireadgroup        none        none
```

Related commands
show snmp-server

snmp-server user

show snmp-server view

Overview This command displays the SNMP server views and is used with SNMP version 3 only.

Syntax
```
show snmp-server view
```

Mode Privileged Exec

Example To display the SNMP server views configured on the device, use the command:

```
awplus# show snmp-server view
```

Output Figure 61-8: Example output from the **show snmp-server view** command

```
SNMP view information:
  View Name ............... view1
    OID ..................... 1
    Type ................... included
```

Related commands show snmp-server

snmp-server view

snmp trap link-status

Overview Use this command to enable SNMP to send link status notifications (traps) for the interfaces when an interface goes up (linkUp) or down (linkDown).

Use the **no** variant of this command to disable the sending of link status notifications.

Syntax

```
snmp trap link-status [enterprise]
no snmp trap link-status
```

Parameter	Description
`enterprise`	Send an Allied Telesis enterprise type of link trap.

Default Disabled

Mode Interface Configuration

Usage notes The link status notifications can be enabled for the following interface types:

- switch port (e.g. port1.0.1)
- VLAN (e.g. vlan2)
- static and dynamic link aggregation (e.g. sa2, po2)

To specify where notifications are sent, use the snmp-server host command. To configure the device globally to send other notifications, use the snmp-server enable trap command.

Examples To enable SNMP to send link status notifications for port1.0.1 to port1.0.3 use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.3
awplus(config-if)# snmp trap link-status
```

To disable the sending of link status notifications for port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
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 port1.0.1 to port1.0.3 after 10 notifications in 40 seconds, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# interface port1.0.1-port1.0.3
```

```
awplus(config-if)# snmp trap link-status suppress time 40
threshold 10
```

To stop suppressing link status notifications for port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no snmp trap link-status suppress
```

Related commands

show interface

snmp trap link-status

snmp-server

Overview Use this command to enable the SNMP agent (server) on the device. The SNMP agent receives and processes SNMP packets sent to the device, and generates notifications (traps) that have been enabled by the snmp-server enable trap command.

Use the **no** variant of this command to disable the SNMP agent on the device. When SNMP is disabled, SNMP packets received by the device are discarded, and no notifications are generated. This does not remove any existing SNMP configuration.

Syntax

```
snmp-server [ip|ipv6]
no snmp-server [ip|ipv6]
```

Parameter	Description
ip	Enable or disable the SNMP agent for IPv4.
ipv6	Enable or disable the SNMP agent for IPv6.

Default By default, the SNMP agent is enabled for both IPv4 and IPv6. If neither the **ip** parameter nor the **ipv6** parameter is specified for this command, then SNMP is enabled or disabled for both IPv4 and IPv6.

Mode Global Configuration

Examples To enable SNMP on the device for both IPv4 and IPv6, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server
```

To enable the SNMP agent for IPv4 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server ip
```

To disable the SNMP agent for both IPv4 and IPv6 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-server
```

To disable the SNMP agent for IPv4, use the commands:

```
awplus(config)# no snmp-server ipv4
```

Related commands

show snmp-server

show snmp-server community

show snmp-server user

snmp-server community

snmp-server contact

snmp-server enable trap

snmp-server engineID local

snmp-server group

snmp-server host

snmp-server location

snmp-server view

snmp-server community

Overview This command creates an SNMP community, optionally setting the access mode for the community. The default access mode is read-only. If view is not specified, the community allows access to all the MIB objects. The SNMP communities are only valid for SNMPv1 and v2c and provide very limited security. Communities should not be used when operating SNMPv3.

The **no** variant of this command removes an SNMP community. The specified community must already exist on the device.

Syntax

```
snmp-server community <community-name> {view
<view-name>|ro|rw|<access-list>}
```

```
no snmp-server community <community-name>
```

Parameter	Description
<community-name>	Community name. The community name is a case sensitive string of up to 20 characters.
`view`	Configure SNMP view. If view is not specified, the community allows access to all the MIB objects.
<view-name>	View name. The view name is a string up to 20 characters long and is case sensitive.
`ro`	Read-only community.
`rw`	Read-write community.
<access-list>	*<1-99>* Access list number.

Mode Global Configuration

Example 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 switch to transmit the specified notifications (traps).

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.
`atmflink`	AMF link traps.
`atmfnode`	AMF node traps.
`atmfrr`	AMF reboot-rolling traps.
`auth`	Authentication failure.
`bgp`	BGP traps.
`chassis`	Chassis traps.
`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 **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.
`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

Parameter	Description
rmon	RMON traps.
thrash-limit	MAC address Thrash Limiting traps.
vcs	VCS traps.
vrrp	Virtual Router Redundancy (VRRP) traps.
ufo	Upstream Forwarding Only (UFO) traps.

Default Disabled

Mode Global Configuration

Usage notes This command cannot be used to enable link status notifications globally. To enable link status notifications for particular interfaces, use the snmp trap link-status command.

To specify where notifications are sent, use the snmp-server host command.

Note that you can enable (or disable) multiple traps with a single command, by specifying a space-separated list of traps.

Examples To enable the device to send a notification if an AMF node changes its status, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap atmfnode
```

To enable the device to send PoE related traps, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap power-inline
```

To disable PoE traps being sent out by the device, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server enable trap power-inline
```

To enable the device to send MAC address Thrash Limiting traps, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap thrash-limit
```

To disable the device from sending MAC address Thrash Limiting traps, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server enable trap thrash-limit
```

To enable the device to send OSPF and VRRP-related traps, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap ospf vrrp
```

To disable OSPF traps being sent out by the device, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server enable trap ospf
```

Related commands

show snmp-server

show ip dhcp snooping

snmp trap link-status

snmp-server host

trap (g8032-switch)

private-vlan ufo trap

Command changes

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.

Mode Global Configuration

Examples To configure the device to send generated traps to the IPv4 host destination 192.0.2.5 with the SNMPv2c community name public, use the following command:

```
awplus# configure terminal
awplus(config)# snmp-server host  version 2c public192.0.2.5
```

To configure the device to send generated traps to the IPv6 host destination 2001:db8::8a2e:7334 with the SNMPv2c community name private, use the following command:

```
awplus# configure terminal
awplus(config)# snmp-server host  version 2c
private2001:db8::8a2e:7334
```

To remove a configured trap host of 192.0.2.5 with the SNMPv2c community name public, use the following command:

```
awplus# configure terminal
awplus(config)# no snmp-server host  version 2c public192.0.2.5
```

Related commands

snmp trap link-status

snmp-server enable trap

snmp-server view

snmp-server 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 vlan2 to be the interface whose IP address is used as the originating address in SNMP informs packets.

```
awplus# configure terminal
awplus(config)# snmp-server source-interface informs vlan2
```

The following commands reset the originating source interface for SNMP trap messages to be the default interface (the originating egress interface):

```
awplus# configure terminal
awplus(config)# no snmp-server source-interface traps
```

Validation Commands show running-config

snmp-server startup-trap-delay

Overview Use this command to set the time in seconds after following completion of the device startup sequence before the device sends any SNMP traps (or SNMP notifications).

Use the no variant of this command to restore the default startup delay of 30 seconds.

Syntax

```
snmp-server startup-trap-delay <delay-time>
no snmp-server startup-trap-delay
```

Parameter	Description
<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|sha-256} <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.
`sha-256`	SHA-256 Secure Hash Algorithm. Note: SHA-256 authentication is required in crypto secure-mode.
<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. DES is not available if you enable crypto secure-mode.
`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.

62 LLDP Commands

Introduction

Overview

LLDP and LLDP-MED can be configured using the commands in this chapter, or by using SNMP with the LLDP-MIB and LLDP-EXT-DOT1-MIB (see the Support for Allied Telesis Enterprise MIBs in AlliedWare Plus).

The Voice VLAN feature can be configured using commands in VLAN Commands chapter.

For more information about LLDP, see the LLDP Feature Overview and Configuration Guide.

LLDP can transmit a lot of data about the network. Typically, the network information gathered using LLDP is transferred to a Network Management System by SNMP. For security reasons, we recommend using SNMPv3 for this purpose (see the SNMP Feature Overview and Configuration Guide).

LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static or dynamic channel groups, but not on the channel groups themselves.

Command List

- "clear lldp statistics" on page 3089
- "clear lldp table" on page 3090
- "debug lldp" on page 3091
- "lldp faststart-count" on page 3093
- "lldp holdtime-multiplier" on page 3094
- "lldp management-address" on page 3095
- "lldp med-notifications" on page 3096
- "lldp med-tlv-select" on page 3097
- "lldp non-strict-med-tlv-order-check" on page 3100
- "lldp notification-interval" on page 3101
- "lldp notifications" on page 3102

- "lldp port-number-type" on page 3103
- "lldp reinit" on page 3104
- "lldp run" on page 3105
- "lldp timer" on page 3106
- "lldp tlv-select" on page 3107
- "lldp transmit receive" on page 3109
- "lldp tx-delay" on page 3110
- "location civic-location configuration" on page 3111
- "location civic-location identifier" on page 3115
- "location civic-location-id" on page 3116
- "location coord-location configuration" on page 3117
- "location coord-location identifier" on page 3119
- "location coord-location-id" on page 3120
- "location elin-location" on page 3122
- "location elin-location-id" on page 3123
- "show debugging lldp" on page 3124
- "show lldp" on page 3126
- "show lldp interface" on page 3128
- "show lldp local-info" on page 3130
- "show lldp neighbors" on page 3135
- "show lldp neighbors detail" on page 3137
- "show lldp statistics" on page 3141
- "show lldp statistics interface" on page 3143
- "show location" on page 3145

clear lldp statistics

Overview This command clears all LLDP statistics (packet and event counters) associated with specified ports. If no port list is supplied, LLDP statistics for all ports are cleared.

Syntax

```
clear lldp statistics [interface <port-list>]
```

Parameter	Description
<port-list>	The ports for which the statistics are to be cleared.

Mode Privileged Exec

Examples To clear the LLDP statistics on ports 1.0.1 and 1.0.6, use the command:

```
awplus# clear lldp statistics interface port1.0.1,port1.0.6
```

To clear all LLDP statistics for all ports, use the command:

```
awplus# clear lldp statistics
```

Related commands show lldp statistics

show lldp statistics interface

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

clear lldp table

Overview This command clears the table of LLDP information received from neighbors through specified ports. If no port list is supplied, neighbor information is cleared for all ports.

Syntax

```
clear lldp table [interface <port-list>]
```

Parameter	Description
<port-list>	The ports for which the neighbor information table is to be cleared.

Mode Privileged Exec

Examples To clear the table of neighbor information received on ports 1.0.1 and 1.0.6, use the command:

```
awplus# clear lldp table interface port1.0.1,port1.0.6
```

To clear the entire table of neighbor information received through all ports, use the command:

```
awplus# clear lldp table
```

Related commands show lldp neighbors

debug lldp

Overview This command enables specific LLDP debug for specified ports. When LLDP debugging is enabled, diagnostic messages are entered into the system log. If no port list is supplied, the specified debugging is enabled for all ports.

The **no** variant of this command disables specific LLDP debug for specified ports. If no port list is supplied, the specified debugging is disabled for all ports.

Syntax

```
debug lldp {[rx][rxpkt][tx][txpkt]} [interface [<port-list>]]
debug lldp operation
no debug lldp {[rx][rxpkt][tx][txpkt]} [interface
[<port-list>]]
no debug lldp operation
no debug lldp all
```

Parameter	Description
`rx`	LLDP receive debug.
`rxpkt`	Raw LLDPDUs received in hex format.
`tx`	LLDP transmit debug.
`txpkt`	Raw Tx LLDPDUs transmitted in hex format.
<port-list>	The ports for which debug is to be configured.
`operation`	Debug for LLDP internal operation on the switch.
`all`	Disables all LLDP debugging for all ports.

Default By default no debug is enabled for any ports.

Mode Privileged Exec

Examples To enable debugging of LLDP receive on ports 1.0.1 and 1.0.6, use the command:

```
awplus# debug lldp rx interface port1.0.1,port1.0.6
```

To enable debugging of LLDP transmit with packet dump on all ports, use the command:

```
awplus# debug lldp tx txpkt
```

To disable debugging of LLDP receive on ports 1.0.1 and 1.0.6, use the command:

```
awplus# no debug lldp rx interface port1.0.1,port1.0.6
```

To turn off all LLDP debugging on all ports, use the command:

```
awplus# no debug lldp all
```

Related commands

show debugging lldp

show running-config lldp

terminal monitor

lldp faststart-count

Overview Use this command to set the fast start count for LLDP-MED. The fast start count determines how many fast start advertisements LLDP sends from a port when it starts sending LLDP-MED advertisements from the port, for instance, when it detects a new LLDP-MED capable device.

The **no** variant of this command resets the LLDPD-MED fast start count to the default (3).

Syntax

```
lldp faststart-count <1-10>
no lldp faststart-count
```

Parameter	Description
<1-10>	The number of fast start advertisements to send.

Default The default fast start count is 3.

Mode Global Configuration

Examples To set the fast start count to 5, use the command:

```
awplus# configure terminal
awplus(config)# lldp faststart-count 5
```

To reset the fast start count to the default setting (3), use the command:

```
awplus# configure terminal
awplus(config)# no lldp faststart-count
```

Related commands show lldp

lldp holdtime-multiplier

Overview This command sets the holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) value that is advertised to neighbors.

The **no** variant of this command sets the multiplier back to its default.

Syntax

```
lldp holdtime-multiplier <2-10>
no lldp holdtime-multiplier
```

Parameter	Description
<2-10>	The multiplier factor.

Default The default holdtime multiplier value is 4.

Mode Global Configuration

Usage The Time-To-Live defines the period for which the information advertised to the neighbor is valid. If the Time-To-Live expires before the neighbor receives another update of the information, then the neighbor discards the information from its database.

Examples To set the holdtime multiplier to 2, use the commands:

```
awplus# configure terminal
awplus(config)# lldp holdtime-multiplier 2
```

To set the holdtime multiplier back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp holdtime-multiplier 2
```

Related commands show lldp

lldp management-address

Overview This command sets the IPv4 address to be advertised to neighbors (in the Management Address TLV) via the specified ports. This address will override the default address for these ports.

The **no** variant of this command clears the user-configured management IP address advertised to neighbors via the specified ports. The advertised address reverts to the default.

Syntax

```
lldp management-address <ipaddr>
no lldp management-address
```

Parameter	Description
<ipaddr>	The IPv4 address to be advertised to neighbors, in dotted decimal format. This must be one of the IP addresses already configured on the device.

Default The local loopback interface primary IPv4 address if set, else the primary IPv4 interface address of the lowest numbered VLAN the port belongs to, else the MAC address of the device's baseboard if no VLAN IP addresses are configured for the port.

Mode Interface Configuration

Usage notes To see the management address that will be advertised, use the show lldp interface command or show lldp local-info command.

Examples To set the management address advertised by port1.0.1 and port1.0.2, to be 192.168.1.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# lldp management-address 192.168.1.6
```

To clear the user-configured management address advertised by port1.0.1 and port1.0.2, and revert to using the default address, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# no lldp management-address
```

Related commands show lldp interface

show lldp local-info

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

lldp med-notifications

Overview Use this command to enable LLDP to send LLDP-MED Topology Change Detected SNMP notifications relating to the specified ports. The switch sends an SNMP event notification when a new LLDP-MED compliant IP Telephony device is connected to or disconnected from a port on the switch.

Use the **no** variant of this command to disable the sending of LLDP-MED Topology Change Detected notifications relating to the specified ports.

Syntax

```
lldp med-notifications
no lldp med-notifications
```

Default The sending of LLDP-MED notifications is disabled by default.

Mode Interface Configuration

Examples To enable the sending of LLDP-MED Topology Change Detected notifications relating to ports port1.0.1 and port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# lldp med-notifications
```

To disable the sending of LLDP-MED notifications relating to port1.0.1 and port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# no lldp med-notifications
```

Related commands

lldp notification-interval

lldp notifications

snmp-server enable trap

show lldp interface

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

lldp med-tlv-select

Overview Use this command to enable LLDP-MED Organizationally Specific TLVs for transmission in LLDP advertisements via the specified ports. The LLDP-MED Capabilities TLV must be enabled before any of the other LLDP-MED Organizationally Specific TLVs are enabled.

Use the **no** variant of this command to disable the specified LLDP-MED Organizationally Specific TLVs for transmission in LLDP advertisements via these ports. In order to disable the LLDP-MED Capabilities TLV, you must also disable the rest of these TLVs. Disabling all these TLVs disables LLDP-MED advertisements.

Syntax

```
lldp med-tlv-select [capabilities] [network-policy] [location]
[power-management-ext] [inventory-management]

lldp med-tlv-select all

no lldp med-tlv-select [capabilities] [network-policy]
[location] [power-management-ext] [inventory-management]

no lldp med-tlv-select all
```

Parameter	Description
`capabilities`	LLDP-MED Capabilities TLV. When this is enabled, the MAC/PHY Configuration/Status TLV from IEEE 802.3 Organizationally Specific TLVs is also automatically included in LLDP-MED advertisements, whether or not it has been explicitly enabled by the lldp tlv-select command.
`network-policy`	Network Policy TLV. This TLV is transmitted if Voice VLAN parameters have been configured using the commands: • switchport voice dscp • switchport voice vlan • switchport voice vlan priority
`location`	Location Identification TLV. This TLV is transmitted if location information has been configured using the commands: • location elin-location-id • location civic-location identifier • location civic-location configuration • location coord-location identifier • location coord-location configuration • location elin-location
`power-management-ext`	Extended Power-via-MDI TLV. This TLV is transmitted if the port is PoE capable, and PoE is enabled (power-inline enable command).

Parameter	Description
`inventory-management`	Inventory Management TLV Set, including the following TLVs: • Hardware Revision • Firmware Revision • Software Revision • Serial Number • Manufacturer Name • Model Name • Asset ID
`all`	All LLDP-MED Organizationally Specific TLVs.

Default By default LLDP-MED Capabilities, Network Policy, Location Identification and Extended Power-via-MDI TLVs are enabled. Therefore, if LLDP is enabled using the lldp run command, by default LLDP-MED advertisements are transmitted on ports that detect LLDP-MED neighbors connected to them.

Mode Interface Configuration

Usage notes LLDP-MED TLVs are only sent in advertisements via a port if there is an LLDP-MED-capable device connected to it. To see whether there are LLDP-MED capable devices connected to the ports, use the show lldp neighbors command.

Examples To enable inclusion of the Inventory TLV Set in advertisements transmitted via port1.0.1 and port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# lldp med-tlv-select inventory-management
```

To exclude the Inventory TLV Set in advertisements transmitted via port1.0.1 and port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# no lldp med-tlv-select inventory-management
```

To disable LLDP-MED advertisements transmitted via port1.0.1 and port1.0.2, disable all these TLVs using the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# no lldp med-tlv-select all
```

Related commands

lldp tlv-select

location elin-location-id

location civic-location identifier

location civic-location configuration

location coord-location identifier

location coord-location configuration

location elin-location

show lldp interface

switchport voice dscp

switchport voice vlan

switchport voice vlan priority

Command changes

Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

lldp non-strict-med-tlv-order-check

Overview Use this command to enable non-strict order checking for LLDP-MED advertisements it receives. That is, use this command to enable LLDP to receive and store TLVs from LLDP-MED advertisements even if they do not use standard TLV order.

Use the **no** variant of this command to disable non-strict order checking for LLDP-MED advertisements, that is, to set strict TLV order checking, so that LLDP discards any LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement.

Syntax

```
lldp non-strict-med-tlv-order-check
no lldp non-strict-med-tlv-order-check
```

Default By default TLV non-strict order checking for LLDP-MED advertisements is disabled. That is, strict order checking is applied to LLDP-MED advertisements, according to ANSI/TIA-1057, and LLDP-MED TLVs in non-standard order are discarded.

Mode Global Configuration

Usage notes The ANSI/TIA-1057 specifies standard order for TLVs in LLDP-MED advertisements, and specifies that if LLDP receives LLDP advertisements with non-standard LLDP-MED TLV order, the TLVs in non-standard order should be discarded. This implementation of LLDP-MED follows the standard: it transmits TLVs in the standard order, and by default discards LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement. However, some implementations of LLDP transmit LLDP-MED advertisements with non-standard TLV order. To receive and store the data from these non-standard advertisements, enable non-strict order checking for LLDP-MED advertisements using this command.

Examples To enable strict TLV order checking, use the commands:

```
awplus# configure terminal
awplus(config)# lldp tlv-order-check
```

To disable strict TLV order checking, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp tlv-order-check
```

Related commands show running-config lldp

lldp notification-interval

Overview This command sets the notification interval. This is the minimum interval between LLDP SNMP notifications (traps) of each kind (LLDP Remote Tables Change Notification and LLDP-MED Topology Change Notification).

The **no** variant of this command sets the notification interval back to its default.

Syntax

```
lldp notification-interval <5-3600>
no lldp notification-interval
```

Parameter	Description
<5-3600>	The interval in seconds.

Default The default notification interval is 5 seconds.

Mode Global Configuration

Examples To set the notification interval to 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp notification-interval 20
```

To set the notification interval back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp notification-interval
```

Related commands lldp notifications

show lldp

lldp notifications

Overview This command enables the sending of LLDP SNMP notifications (traps) relating to specified ports.

The **no** variant of this command disables the sending of LLDP SNMP notifications for specified ports.

Syntax

```
lldp notifications
no lldp notifications
```

Default The sending of LLDP SNMP notifications is disabled by default.

Mode Interface Configuration

Examples To enable sending of LLDP SNMP notifications for ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp notifications
```

To disable sending of LLDP SNMP notifications for ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp notifications
```

Related commands

lldp notification-interval

show lldp interface

snmp-server enable trap

lldp port-number-type

Overview This command sets the type of port identifier used to enumerate, that is to count, the LLDP MIB local port entries. The LLDP MIB (IEEE Standard 802.1AB-2005, Section 12, LLDP MIB Definitions.) requires the port number value to count LLDP local port entries.

This command also enables you to optionally set an interface index to enumerate the LLDP MIB local port entries, if required by your management system.

The **no** variant of this command resets the type of port identifier back to the default setting (number).

Syntax

```
lldp port-number-type [number|ifindex]
no lldp port-number-type
```

Parameter	Description
`number`	Set the type of port identifier to a port number to enumerate the LLDP MIB local port entries.
`ifindex`	Set the type of port identifier to an interface index to enumerate the LLDP MIB local port entries.

Default The default port identifier type is number. The no variant of this command sets the port identifier type to the default.

Mode Global Configuration

Examples To set the type of port identifier used to enumerate LLDP MIB local port entries to port numbers, use the commands:

```
awplus# configure terminal
awplus(config)# lldp port-number-type number
```

To set the type of port identifier used to enumerate LLDP MIB local port entries to interface indexes, use the commands:

```
awplus# configure terminal
awplus(config)# lldp port-number-type ifindex
```

To reset the type of port identifier used to enumerate LLDP MIB local port entries the default (port numbers), use the commands:

```
awplus# configure terminal
awplus(config)# no lldp port-number-type
```

Related commands show lldp

lldp reinit

Overview This command sets the value of the reinitialization delay. This is the minimum time after disabling LLDP on a port before it can reinitialize.

The **no** variant of this command sets the reinitialization delay back to its default setting.

Syntax

```
lldp reinit <1-10>
no lldp reinit
```

Parameter	Description
<1-10>	The delay in seconds.

Default The default reinitialization delay is 2 seconds.

Mode Global Configuration

Examples To set the reinitialization delay to 3 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp reinit 3
```

To set the reinitialization delay back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp reinit
```

Related commands show lldp

lldp run

Overview This command enables the operation of LLDP on the device.

The **no** variant of this command disables the operation of LLDP on the device. The LLDP configuration remains unchanged.

Syntax

```
lldp run
no lldp run
```

Default LLDP is disabled by default.

Mode Global Configuration

Examples To enable LLDP operation, use the commands:

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

To disable LLDP operation, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp run
```

Related commands show lldp

lldp timer

Overview This command sets the value of the transmit interval. This is the interval between regular transmissions of LLDP advertisements.

The **no** variant of this command sets the transmit interval back to its default.

Syntax

```
lldp timer <5-32768>
no lldp timer
```

Parameter	Description
<5-32768>	The transmit interval in seconds. The transmit interval must be at least four times the transmission delay timer (lldp tx-delay command).

Default The default transmit interval is 30 seconds.

Mode Global Configuration

Examples To set the transmit interval to 90 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp timer 90
```

To set the transmit interval back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp timer
```

Related commands lldp tx-delay

show lldp

lldp tlv-select

Overview This command enables one or more optional TLVs, or all TLVs, for transmission in LLDP advertisements via the specified ports. The TLVs can be specified in any order; they are placed in LLDP frames in a fixed order (as described in IEEE 802.1AB). The mandatory TLVs (Chassis ID, Port ID, Time To Live, End of LLDPDU) are always included in LLDP advertisements.

In LLDP-MED advertisements the MAC/PHY Configuration/Status TLV will be always be included regardless of whether it is selected by this command.

The **no** variant of this command disables the specified optional TLVs, or all optional TLVs, for transmission in LLDP advertisements via the specified ports.

Syntax

```
lldp tlv-select {[<tlv>]...}
lldp tlv-select all
no lldp tlv-select {[<tlv>]...}
no lldp tlv-select all
```

Parameter	Description
`<tlv>`	The TLV to transmit in LLDP advertisements. One of these keywords: • port-description (specified by the description (interface) command) • system-name (specified by the hostname command) • system-description • system-capabilities • management-address • port-vlan • port-and-protocol-vlans • vlan-names • protocol-ids • mac-phy-config • power-management (Power Via MDI TLV) • link-aggregation • max-frame-size
`all`	All TLVs.

Default By default no optional TLVs are included in LLDP advertisements. The MAC/PHY Configuration/Status TLV (**mac-phy-config**) is included in LLDP-MED advertisements whether or not it is selected by this command.

Mode Interface Configuration

Examples

To include the management-address and system-name TLVs in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp tlv-select management-address
system-name
```

To include all optional TLVs in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp tlv-select all
```

To exclude the management-address and system-name TLVs from advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp tlv-select management-address
system-name
```

To exclude all optional TLVs from advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp tlv-select all
```

Related commands

description (interface)

hostname

lldp med-tlv-select

show lldp interface

show lldp local-info

lldp transmit receive

Overview This command enables transmission and/or reception of LLDP advertisements to or from neighbors through the specified ports.

The **no** variant of this command disables transmission and/or reception of LLDP advertisements through specified ports.

Syntax

```
lldp {[transmit] [receive]}
no lldp {[transmit] [receive]}
```

Parameter	Description
`transmit`	Enable or disable transmission of LLDP advertisements via this port or ports.
`receive`	Enable or disable reception of LLDP advertisements via this port or ports.

Default LLDP advertisement transmission and reception are enabled on all ports by default.

Mode Interface Configuration

Examples To enable transmission of LLDP advertisements on port1.0.1 and port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# lldp transmit
```

To enable LLDP advertisement transmission and reception on port1.0.1 and port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# lldp transmit receive
```

To disable LLDP advertisement transmission and reception on port1.0.1 and port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.2
awplus(config-if)# no lldp transmit receive
```

Related commands show lldp interface

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

lldp tx-delay

Overview This command sets the value of the transmission delay timer. This is the minimum time interval between transmitting LLDP advertisements due to a change in LLDP local information.

The **no** variant of this command sets the transmission delay timer back to its default setting.

Syntax

```
lldp tx-delay <1-8192>
no lldp tx-delay
```

Parameter	Description
<1-8192>	The transmission delay in seconds. The transmission delay cannot be greater than a quarter of the transmit interval (lldp timer command).

Default The default transmission delay timer is 2 seconds.

Mode Global Configuration

Examples To set the transmission delay timer to 12 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp tx-delay 12
```

To set the transmission delay timer back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp tx-delay
```

Related commands lldp timer

show lldp

location civic-location configuration

Overview Use these commands to configure a civic address location. The country parameter must be specified first, and at least one of the other parameters must be configured before the location can be assigned to a port.

Use the **no** variants of this command to delete civic address parameters from the location.

Syntax

```
country <country>
state <state>
no state
county <county>
no county
city <city>
no city
division <division>
no division
neighborhood <neighborhood>
no neighborhood
street-group <street-group>
no street-group
leading-street-direction <leading-street-direction>
no leading-street-direction
trailing-street-suffix <trailing-street-suffix>
no trailing-street-suffix
street-suffix <street-suffix>
no street-suffix
house-number <house-number>
no house-number
house-number-suffix <house-number-suffix>
no house-number-suffix
landmark <landmark>
no landmark
additional-information <additional-information>
no additional-information
```

Syntax (cont.)

```
name <name>
no name
postalcode <postalcode>
no postalcode
building <building>
no building
unit <unit>
no unit
floor <floor>
no floor
room <room>
no room
place-type <place-type>
no place-type
postal-community-name <postal-community-name>
no postal-community-name
post-office-box <post-office-box>
no post-office-box
additional-code <additional-code>
no additional-code
seat <seat>
no seat
primary-road-name <primary-road-name>
no primary-road-name
road-section <road-section>
no road-section
branch-road-name <branch-road-name>
no branch-road-name
sub-branch-road-name <sub-branch-road-name>
no sub-branch-road-name
street-name-pre-modifier <street-name-pre-modifier>
no street-name-pre-modifier
streetname-post-modifier <streetname-post-modifier>
no streetname-post-modifier
```

Parameter	Description
<country>	Upper-case two-letter country code, as specified in ISO 3166.
<state>	State (Civic Address (CA) Type 1): national subdivisions (state, canton, region).
<county>	County (CA Type 2): County, parish, gun (JP), district (IN).
<city>	City (CA Type 3): city, township, shi (JP).
<division>	City division (CA Type 4): City division, borough, city district, ward, chou (JP).
<neighborhood>	Neighborhood (CA Type 5): neighborhood, block.
<street-group>	Street group (CA Type 6): group of streets below the neighborhood level.
<leading-street-direction>	Leading street direction (CA Type 16).
<trailing-street-suffix>	Trailing street suffix (CA Type 17).
<street-suffix>	Street suffix (CA Type 18): street suffix or type.
<house-number>	House number (CA Type 19).
<house-number-suffix>	House number suffix (CA Type 20).
<landmark>	Landmark or vanity address (CA Type 21).
<additional-information>	Additional location information (CA Type 22).
<name>	Name (CA Type 23): residence and office occupant.
<postal-code>	Postal/zip code (CA Type 24).
<building>	Building (CA Type 25): structure.
<unit>	Unit (CA Type 26): apartment, suite.
<floor>	Floor (CA Type 27).
<room>	Room (CA Type 28).
<place-type>	Type of place (CA Type 29).
<postal-community-name>	Postal community name (CA Type 30).
<post-office-box>	Post office box (P.O. Box) (CA Type 31).
<additional-code>	Additional code (CA Type 32).
<seat>	Seat (CA Type 33): seat (desk, cubicle, workstation).
<primary-road-name>	Primary road name (CA Type 34).
<road-section>	Road section (CA Type 35).

Parameter	Description
<branch-road-name>	Branch road name (CA Type 36).
<sub-branch-road-name>	Sub-branch road name (CA Type 37).
<street-name-pre-modifier>	Street name pre-modifier (CA Type 38).
<street-name-post-modifier>	Street name post-modifier (CA Type 39).

Default By default no civic address location information is configured.

Mode Civic Address Location Configuration

Usage notes The **country** parameter must be configured before any other parameters can be configured; this creates the location. The country parameter cannot be deleted. One or more of the other parameters must be configured before the location can be assigned to a port. The country parameter must be entered as an upper-case two-letter country code, as specified in ISO 3166. All other parameters are entered as alpha-numeric strings. Do not configure all the civic address parameters (this would generate TLVs that are too long). Configure a subset of these parameters—enough to consistently and precisely identify the location of the device. If the location is to be used for Emergency Call Service (ECS), the particular ECS application may have guidelines for configuring the civic address location. For more information about civic address format, see the LLDP Feature Overview and Configuration Guide.

To specify the civic address location, use the location civic-location identifier command. To delete the civic address location, use the **no** variant of the **location civic-location identifier** command. To assign the civic address location to particular ports, so that it can be advertised in TLVs from those ports, use the command location civic-location-id command.

Examples To configure civic address location 1 with location "27 Nazareth Avenue, Christchurch, New Zealand" in civic-address format, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)# country NZ
awplus(config-civic)# city Christchurch
awplus(config-civic)# primary-road-name Nazareth
awplus(config-civic)# street-suffix Avenue
awplus(config-civic)# house-number 27
```

Related commands location civic-location-id

location civic-location identifier

show lldp local-info

show location

location civic-location identifier

Overview Use this command to enter the Civic Address Location Configuration mode to configure the specified location.

Use the **no** variant of this command to delete a civic address location. This also removes the location from any ports it has been assigned to.

Syntax

```
location civic-location identifier <civic-loc-id>
no location civic-location identifier <civic-loc-id>
```

Parameter	Description
<civic-loc-id>	A unique civic address location ID, in the range 1 to 4095.

Default By default there are no civic address locations.

Mode Global Configuration

Usage notes To configure the location information for this civic address location identifier, use the location civic-location configuration command. To associate this civic location identifier with particular ports, use the location elin-location-id command.

Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

Examples To enter Civic Address Location Configuration mode for the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)#
```

To delete the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location civic-location identifier 1
```

Related commands

location civic-location-id

location civic-location configuration

show location

show running-config lldp

location civic-location-id

Overview Use this command to assign a civic address location to the ports. The civic address location must already exist. This replaces any previous assignment of civic address location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location identifier from the ports.

Syntax

```
location civic-location-id <civic-loc-id>
no location civic-location-id [<civic-loc-id>]
```

Parameter	Description
<civic-loc-id>	Civic address location ID, in the range 1 to 4095.

Default By default no civic address location is assigned to ports.

Mode Interface Configuration

Usage notes The civic address location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, create the location using the following commands:

- location civic-location identifier command
- location civic-location configuration command

If a civic-address location is deleted using the **no** variant of the location civic-location identifier command, it is automatically removed from all ports.

Examples To assign the civic address location 1 to port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location civic-location-id 1
```

To remove a civic address location from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location civic-location-id
```

Related commands

lldp med-tlv-select

location civic-location identifier

location civic-location configuration

show location

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

location coord-location configuration

Overview Use this command to configure a coordinate-based location. All parameters must be configured before assigning this location identifier to a port.

Syntax

```
latitude <latitude>
lat-resolution <lat-resolution>
longitude <longitude>
long-resolution <long-resolution>
altitude <altitude> {meters|floor}
alt-resolution <alt-resolution>
datum {wgs84|nad83-navd|nad83-mllw}
```

Parameter	Description
<lat-resolution>	Latitude resolution, as a number of valid bits, in the range 0 to 34.
<latitude>	Latitude value in degrees in the range -90.0 to 90.0
<long-resolution>	Longitude resolution, as a number of valid bits, in the range 0 to 34.
<longitude>	Longitude value in degrees, in the range -180.0 to 180.0.
<alt-resolution>	Altitude resolution, as a number of valid bits, in the range 0 to 30. A resolution of 0 can be used to indicate an unknown value.
<altitude>	Altitude value, in meters or floors.
`meters`	The altitude value is in meters.
`floors`	The altitude value is in floors.
`datum`	The geodetic system (or datum) that the specified coordinate values are based on.
`wgs84`	World Geodetic System 1984.
`nad83-navd`	North American Datum 1983 - North American Vertical Datum.
`nad83-mllw`	North American Datum 1983 - Mean Lower Low Water vertical datum.

Default By default no coordinate location information is configured.

Mode Coordinate Configuration

Usage Latitude and longitude values are always stored internally, and advertised in the Location Identification TLV, as 34-bit fixed-point binary numbers, with a 25-bit fractional part, irrespective of the number of digits entered by the user. Likewise

altitude is stored as a 30- bit fixed point binary number, with an 8-bit fractional part. Because the user-entered decimal values are stored as fixed point binary numbers, they cannot always be represented exactly—the stored binary number is converted to a decimal number for display in the output of the show location command. For example, a user-entered latitude value of "2.77" degrees is displayed as "2.76999998092651367187500000".

The **lat-resolution**, **long-resolution**, and **alt-resolution** parameters allow the user to specify the resolution of each coordinate element as the number of valid bits in the internally-stored binary representation of the value. These resolution values can be used by emergency services to define a search area.

To specify the coordinate identifier, use the location coord-location identifier command. To remove coordinate information, delete the coordinate location by using the **no** variant of that command. To associate the coordinate location with particular ports, so that it can be advertised in TLVs from those ports, use the location elin-location-id command.

Example To configure the location for the White House in Washington DC, which has the coordinates based on the WGS84 datum of 38.89868 degrees North (with 22 bit resolution), 77.03723 degrees West (with 22 bit resolution), and 15 meters height (with 9 bit resolution), use the commands:

```
awplus# configure terminal
awplus(config)# location coord-location identifier 1
awplus(config-coord)# la-resolution 22
awplus(config-coord)# latitude 38.89868
awplus(config-coord)# lo-resolution 22
awplus(config-coord)# longitude -77.03723
awplus(config-coord)# alt-resolution 9
awplus(config-coord)# altitude 15 meters
awplus(config-coord)# datum wgs84
```

Related commands

location coord-location-id

location coord-location identifier

show lldp local-info

show location

location coord-location identifier

Overview Use this command to enter Coordinate Location Configuration mode for this coordinate location.

Use the **no** variant of this command to delete a coordinate location. This also removes the location from any ports it has been assigned to.

Syntax

```
location coord-location identifier <coord-loc-id>
no location coord-location identifier <coord-loc-id>
```

Parameter	Description
<coord-loc-id>	A unique coordinate location identifier, in the range 1 to 4095.

Default By default there are no coordinate locations.

Mode Global Configuration

Usage Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

To configure this coordinate location, use the location coord-location configuration command. To associate this coordinate location with particular ports, so that it can be advertised in TLVs from those ports, use the location coord-location-id command.

Examples To enter Coordinate Location Configuration mode to configure the coordinate location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# location coord-location identifier 1
awplus(config-coord)#
```

To delete coordinate location 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location coord-location identifier 1
```

Related commands

location coord-location-id

location coord-location configuration

show lldp local-info

show location

location coord-location-id

Overview Use this command to assign a coordinate location to the ports. The coordinate location must already exist. This replaces any previous assignment of coordinate location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location from the ports.

Syntax

```
location coord-location-id <coord-loc-id>
no location coord-location-id [<coord-loc-id>]
```

Parameter	Description
<coord-loc-id>	Coordinate location ID, in the range 1 to 4095.

Default By default no coordinate location is assigned to ports.

Mode Interface Configuration

Usage notes The coordinate location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, configure the location using the following commands:

- location coord-location identifier command
- location coord-location configuration command

If a coordinate location is deleted using the **no** variant of the location coord-location identifier command, it is automatically removed from all ports.

Examples To assign coordinate location 1 to port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location coord-location-id 1
```

To remove a coordinate location from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location coord-location-id
```

Related commands

lldp med-tlv-select

location coord-location identifier

location coord-location configuration

show location

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

location elin-location

Overview Use this command to create or modify an ELIN location.

Use the **no** variant of this command to delete an ELIN location, and remove it from any ports it has been assigned to.

Syntax

```
location elin-location <elin> identifier <elin-loc-id>
no location elin-location identifier <elin-loc-id>
```

Parameter	Description
<elin>	Emergency Location Identification Number (ELIN) for Emergency Call Service (ECS), in the range 10 to 25 digits long. In North America, ELINs are typically 10 digits long.
<elin-loc-id>	A unique ELIN location identifier, in the range 1 to 4095.

Default By default there are no ELIN location identifiers.

Mode Global Configuration

Usage Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

To assign this ELIN location to particular ports, so that it can be advertised in TLVs from those ports, use the location elin-location-id command.

Examples To create a new ELIN location with ID 1, and configure it with ELIN "1234567890", use the commands:

```
awplus# configure terminal
awplus(config)# location elin-location 1234567890 identifier 1
```

To delete existing ELIN location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location elin-location identifier 1
```

Related commands

location elin-location-id

show lldp local-info

show location

location elin-location-id

Overview Use this command to assign an ELIN location to the ports. The ELIN location must already exist. This replaces any previous assignment of ELIN location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location identifier from the ports.

Syntax

```
location elin-location-id <elin-loc-id>
no location elin-location-id [<elin-loc-id>]
```

Parameter	Description
<elin-loc-id>	ELIN location identifier, in the range 1 to 4095.

Default By default no ELIN location is assigned to ports.

Mode Interface Configuration

Usage notes An ELIN location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, configure the location using the location elin-location command.

If an ELIN location is deleted using the **no** variant of one of the location elin-location command, it is automatically removed from all ports.

Examples To assign ELIN location 1 to port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location elin-location-id 1
```

To remove ELIN location 1 from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location elin-location-id 1
```

Related commands lldp med-tlv-select

location elin-location

show location

Command changes Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

show debugging lldp

Overview This command displays LLDP debug settings for specified ports. If no port list is supplied, LLDP debug settings for all ports are displayed.

Syntax

```
show debugging lldp [interface <port-list>]
```

Parameter	Description
<port-list>	The ports for which the LLDP debug settings are shown.

Mode User Exec and Privileged Exec

Examples To display LLDP debug settings for all ports, use the command:

```
awplus# show debugging lldp
```

To display LLDP debug settings for ports 1.0.1 to 1.0.6, use the command:

```
awplus# show debugging lldp interface port1.0.1-1.0.6
```

Output Figure 62-1: Example output from the **show debugging lldp** command

```
LLDP Debug settings:
Debugging for LLDP internal operation is on
Port       Rx    RxPkt   Tx    TxPkt
-----------------------------------
1.0.1      Yes   Yes     No    No
1.0.2      Yes   No      No    No
1.0.3      No    No      No    No
1.0.4      Yes   Yes     Yes   No
1.0.5      Yes   No      Yes   No
1.0.6      Yes   Yes     Yes   Yes
```

Table 1: Parameters in the output of the **show debugging lldp** command

Parameter	Description
Port	Port name.
Rx	Whether debugging of LLDP receive is enabled on the port.
RxPkt	Whether debugging of LLDP receive packet dump is enabled on the port.
Rx	Whether debugging of LLDP transmit is enabled on the port.
RxPkt	Whether debugging of LLDP transmit packet dump is enabled on the port.

Related commands debug lldp

show lldp

Overview This command displays LLDP status and global configuration settings.

Syntax

```
show lldp
```

Mode User Exec and Privileged Exec

Example To display LLDP status and global configuration settings, use the command:

```
awplus# show lldp
```

Output

Table 2: Example output from the **show lldp** command

```
awplus# show lldp

LLDP Global Configuration:              [Default Values]
LLDP Status ............... Enabled     [Disabled]
Notification Interval ..... 5 secs      [5]
Tx Timer Interval ......... 30 secs     [30]
Hold-time Multiplier ...... 4           [4]
(Computed TTL value ....... 120 secs)
Reinitialization Delay .... 2 secs      [2]
Tx Delay .................. 2 secs      [2]

Port Number Type........... Ifindex     [Port-Number]
Fast Start Count .......... 5           [3]

LLDP Global Status:
Total Neighbor Count ...... 47
Neighbors table last updated 0 hrs 0 mins 43 secs ago
```

Table 3: Parameters in the output of the **show lldp** command

Parameter	Description
LLDP Status	Whether LLDP is enabled. Default is disabled.
Notification Interval	Minimum interval between LLDP notifications.
Tx Timer Interval	Transmit interval between regular transmissions of LLDP advertisements.
Hold-time Multiplier	The holdtime multiplier. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) value that is advertised to neighbors.
Reinitialization Delay	The reinitialization delay. This is the minimum time after disabling LLDP transmit on a port before it can reinitialize again.

Table 3: Parameters in the output of the **show lldp** command (cont.)

Parameter	Description
`Tx Delay`	The transmission delay. This is the minimum time interval between transmitting advertisements due to a change in LLDP local information.
`Port Number Type`	The type of port identifier used to enumerate LLDP MIB local port entries, as set by the lldp port-number-type command.
`Fast Start Count`	The number of times fast start advertisements are sent for LLDP-MED.
`Total Neighbor Count`	Number of LLDP neighbors discovered on all ports.
`Neighbors table last updated`	The time since the LLDP neighbor table was last updated.

Related commands

show lldp interface

show running-config lldp

show lldp interface

Overview This command displays LLDP configuration settings for specified ports. If no port list is specified, LLDP configuration for all ports is displayed.

Syntax

```
show lldp interface [<port-list>]
```

Parameter	Description
<port-list>	The ports for which the LLDP configuration settings are to be shown.

Mode User Exec and Privileged Exec

Examples To display LLDP configuration settings for ports 1.0.1 to 1.0.6, use the command:

```
awplus# show lldp interface port1.0.1-1.0.6
```

To display LLDP configuration settings for all ports, use the command:

```
awplus# show lldp interface
```

Output Figure 62-2: Example output from the **show lldp interface** command

```
awplus# show lldp interface port1.0.1-1.0.8
LLDP Port Status and Configuration:

  * = LLDP is inactive on this port because it is a mirror analyser port
  Notification Abbreviations:
    RC = LLDP Remote Tables Change       TC = LLDP-MED Topology Change
  TLV Abbreviations:
    Base:  Pd = Port Description         Sn = System Name
           Sd = System Description       Sc = System Capabilities
           Ma = Management Address
    802.1: Pv = Port VLAN ID             Pp = Port And Protocol VLAN ID
           Vn = VLAN Name                Pi = Protocol Identity
    802.3: Mp = MAC/PHY Config/Status    Po = Power Via MDI (PoE)
           La = Link Aggregation         Mf = Maximum Frame Size
    MED:   Mc = LLDP-MED Capabilities    Np = Network Policy
           Lo = Location Identification  Pe = Extended PoE    In = Inventory

                                          Optional TLVs Enabled for Tx
 Port     Rx/Tx  Notif  Management Addr  Base       802.1    802.3    MED
-------------------------------------------------------------------------------
 1.0.1    Rx Tx  RC --  192.168.100.123  PdSnSdScMa -------- -------- McNpLoPe--
*1.0.2    -- Tx  RC --  192.168.100.123  PdSnSdScMa -------- -------- McNpLoPe--
 1.0.3    Rx Tx  RC --  192.168.100.123  Pd--SdScMa PvPpVnPi -------- McNpLoPe--
 1.0.4    -- --  RC --  192.168.100.123  PdSnSd--Ma -------- -------- McNpLoPe--
 1.0.5    Rx Tx  RC TC  192.168.100.123  PdSnSdScMa PvPpVnPi -------- McNpLoPe--
 1.0.6    Rx Tx  RC TC  192.168.100.123  Pd----ScMa -------- -------- McNpLoPe--
 1.0.7    Rx Tx  -- TC  192.168.100.123  PdSnSdScMa PvPpVnPi MpPoLaMf McNpLoPeIn
 1.0.8    Rx Tx  -- TC  192.168.1.1      PdSn--ScMa PvPpVnPi -------- McNp------
```

Table 4: Parameters in the output of the **show lldp interface** command

Parameter	Description
`Port`	Port name.
`Rx`	Whether reception of LLDP advertisements is enabled on the port.
`Tx`	Whether transmission of LLDP advertisements is enabled on the port.
`Notif`	Whether sending SNMP notification for LLDP is enabled on the port: • RM = Remote Tables Change Notification • TP = LLDP-MED Topology Change Notification
`Management Addr`	Management address advertised to neighbors.
`Base TLVs Enabled for Tx`	List of optional Base TLVs enabled for transmission: • Pd = Port Description • Sn =System Name • Sd = System Description • Sc =System Capabilities • Ma = Management Address
`802.1 TLVs Enabled for Tx`	List of optional 802.1 TLVs enabled for transmission: • Pv = Port VLAN ID • Pp = Port And Protocol VLAN ID • Vn = VLAN Name • Pi =Protocol Identity
`802.3 TLVs Enabled for Tx`	List of optional 802.3 TLVs enabled for transmission: • Mp = MAC/PHY Configuration/Status • Po = Power Via MDI (PoE) • La = Link Aggregation • Mf = Maximum Frame Size
`MED TLVs Enabled for Tx`	List of optional LLDP-MED TLVs enabled for transmission: • Mc = LLDP-MED Capabilities • Np = Network Policy • Lo = Location Information, • Pe = Extended Power-Via-MDI • In = Inventory

Related commands

show lldp

show running-config lldp

show lldp local-info

Overview This command displays local LLDP information that can be transmitted through specified ports. If no port list is entered, local LLDP information for all ports is displayed.

Syntax

```
show lldp local-info [base] [dot1] [dot3] [med] [interface
<port-list>]
```

Parameter	Description
`base`	Information for base TLVs.
`dot1`	Information for 802.1 TLVs.
`dot3`	Information for 802.3 TLVs.
`med`	Information for LLDP-MED TLVs.
<port-list>	The ports for which the local information is to be shown.

Mode User Exec and Privileged Exec

Usage notes Whether and which local information is transmitted in advertisements via a port depends on:

- whether the port is set to transmit LLDP advertisements (lldp transmit receive command)
- which TLVs it is configured to send (lldp tlv-select command, lldp med-tlv-select command)

Examples To display local information transmitted via port 1.0.1, use the command:

```
awplus# show lldp local-info interface port1.0.1
```

To display local information transmitted via all ports, use the command:

```
awplus# show lldp local-info
```

Output Figure 62-3: Example output from **show lldp local-info**

```
LLDP Local Information:

Local port1.0.1:
  Chassis ID Type ................... MAC address
  Chassis ID ........................ 0015.77c9.7453
  Port ID Type ...................... Interface alias
  Port ID ........................... port1.0.1
  TTL ............................... 120
  Port Description .................. [not configured]
```

```
System Name ..................... awplus
System Description .............. Allied Telesis router/switch, AW+
                                  v5.4.6
System Capabilities - Supported .. Bridge, Router
                    - Enabled .... Bridge, Router
Management Address .............. 192.168.1.6
Port VLAN ID (PVID) ............. 1
Port & Protocol VLAN - Supported . Yes
                     - Enabled ... No
                     - VIDs ..... 0
VLAN Names ...................... default
Protocol IDs .................... 9000, 0026424203000000, 888e01, aaaa03,
                                  88090101, 00540000e302, 0800, 0806, 86dd
MAC/PHY Auto-negotiation ........ Supported, Enabled
     Advertised Capability ...... 1000BaseTFD, 100BaseTXFD, 100BaseTX,
                                  10BaseTFD, 10BaseT
     Operational MAU Type ....... 1000BaseTFD (30)
Power Via MDI (PoE) ............. Supported, Enabled
     Port Class ................. PSE
     Pair Control Ability ....... Disabled
     Power Class ................ Unknown
Link Aggregation ................ Supported, Disabled
Maximum Frame Size .............. 1522
LLDP-MED Device Type ............ Network Connectivity
LLDP-MED Capabilities ........... LLDP-MED Capabilities, Network Policy,
                                  Location Identification,
                                  Extended Power - PSE, Inventory
Network Policy .................. [not configured]
Location Identification ......... Civic Address
     Country Code ............... NZ
     City ....................... Christchurch
     Street Suffix .............. Avenue
     House Number ............... 27
     Primary Road Name .......... Nazareth
Location Identification ......... ELIN
     ELIN ....................... 123456789012
LLDP-MED Device Type ............ Network Connectivity
LLDP-MED Capabilities ........... LLDP-MED Capabilities, Network Policy,
                                  Location Identification,
                                  Extended Power - PSE, Inventory
Extended Power Via MDI (PoE) ..... PSE
     Power Source ............... Primary Power
     Power Priority ............. Low
     Power Value ................ 4.4 Watts
Inventory Management:
     Hardware Revision .......... A-0
     Firmware Revision .......... 1.1.0
     Software Revision .......... v5.4.6
     Serial Number .............. G1Q78900B
     Manufacturer Name .......... Allied Telesis Inc.
     Model Name ................. AT-x930-52GPX
     Asset ID ................... [zero length]
```

Table 62-1: Parameters in the output of **show lldp local-info**

Parameter	Description
`Chassis ID Type`	Type of the Chassis ID.
`Chassis ID`	Chassis ID that uniquely identifies the local device.
`Port ID Type`	Type of the Port ID.
`Port ID`	Port ID of the local port through which advertisements are sent.
`TTL`	Number of seconds that the information advertised by the local port remains valid.
`Port Description`	Port description of the local port, as specified by the description (interface) command.
`System Name`	System name, as specified by the hostname command.
`System Description`	System description.
`System Capabilities (Supported)`	Capabilities that the local port supports.
`System Capabilities (Enabled)`	Enabled capabilities on the local port.
`Management Addresses`	Management address associated with the local port. To change this, use the lldp management-address command.
`Port VLAN ID (PVID)`	VLAN identifier associated with untagged or priority tagged frames received via the local port.
`Port & Protocol VLAN (Supported)`	Whether Port & Protocol VLANs (PPV) is supported on the local port.
`Port & Protocol VLAN (Enabled)`	Whether the port is in one or more Port & Protocol VLANs.
`Port & Protocol VLAN (VIDs)`	List of identifiers for Port & Protocol VLANs that the port is in.
`VLAN Names`	List of VLAN names for VLANs that the local port is assigned to.
`Protocol IDs`	List of protocols that are accessible through the local port.
`MAC/PHY Auto-negotiation`	Auto-negotiation support and current status of the 802.3 LAN on the local port.

Table 62-1: Parameters in the output of **show lldp local-info** (cont.)

Parameter	Description
`Power Via MDI (PoE)`	PoE-capability and current status on the local port.
`Port Class`	Whether the device is a PSE (Power Sourcing Entity) or a PD (Powered Device)
`Pair Control Ability`	Whether power pair selection can be controlled
`Power Pairs`	Which power pairs are selected for power ("Signal Pairs" or "Spare Pairs") if pair selection can be controlled
`Power Class`	The power class of the PD device on the port (class 0, 1, 2, 3 or 4)
`Link Aggregation`	Whether the link is capable of being aggregated and it is currently in an aggregation.
`Aggregated Port-ID`	Aggregated port identifier.
`Maximum Frame Size`	The maximum frame size capability of the implemented MAC and PHY.
`LLDP-MED Device Type`	LLDP-MED device type
`LLDP-MED Capabilities`	Capabilities LLDP-MED capabilities supported on the local port.
`Network Policy`	List of network policies configured on the local port.
`VLAN ID`	VLAN identifier for the port for the specified application type
`Tagged Flag`	Whether the VLAN ID is to be used as tagged or untagged
`Layer-2 Priority:`	Layer 2 User Priority (in the range 0 to 7)
`DSCP Value`	Diffserv codepoint (in the range 0 to 63)
`Location Identification`	Location configured on the local port.
`Extended Power Via MDI (PoE)`	PoE-capability and current status of the PoE parameters for Extended Power-Via-MDI TLV on the local port.
`Power Source`	The power source the switch currently uses; either primary power or backup power.
`Power Priority`	The power priority configured on the port; either critical, high or low.

Table 62-1: Parameters in the output of **show lldp local-info** (cont.)

Parameter	Description
`Power Value`	The total power the switch can source over a maximum length cable to a PD device on the port. The value shows the power value in Watts from the PD side.
`Inventory Management`	Inventory information for the device.

Related commands

description (interface)

hostname

lldp transmit receive

show lldp neighbors

Overview This command displays a summary of information received from neighbors via specified ports. If no port list is supplied, neighbor information for all ports is displayed.

Syntax

```
show lldp neighbors [interface <port-list>]
```

Parameter	Description
<port-list>	The ports for which the neighbor information is to be shown.

Mode User Exec and Privileged Exec

Examples To display neighbor information received via all ports, use the command:

```
awplus# show lldp neighbors
```

To display neighbor information received via ports 1.0.1 and 1.0.6 with LLDP-MED configuration, use the command:

```
awplus# show lldp neighbors interface port1.0.1,port1.0.6
```

Output Figure 62-4: Example output from the **show lldp neighbors** command

```
LLDP Neighbor Information:

Total number of neighbors on these ports .... 4

  System Capability Codes:
    O = Other    P = Repeater   B = Bridge                W = WLAN Access Point
    R = Router   T = Telephone  C = DOCSIS Cable Device   S = Station Only
  LLDP-MED Device Type and Power Source Codes:
    1 = Class I    3 = Class III    PSE  = PoE    Both = PoE&Local   Prim = Primary
    2 = Class II   N = Network Con. Locl = Local  Unkn = Unknown     Back = Backup

Local    Neighbor        Neighbor        Neighbor                System      MED
Port     Chassis ID      Port ID         Sys Name                Cap.        Ty Pwr
-------------------------------------------------------------------------------
1.0.1    002d.3044.7ba6  port1.0.2       awplus                  OPBWRTCS
1.0.1    0011.3109.e5c6  port1.0.3       AT-9924 switch/route... --B-R---
1.0.6    0000.10cf.8590  port3           AR-442S                 --B-R---
1.0.6    00ee.4352.df51  192.168.1.2     Jim's desk phone        --B--T--    3  PSE
```

Table 63: Parameters in the output of the **show lldp neighbors** command

Parameter	Description
`Local Port`	Local port on which the neighbor information was received.
`Neighbor Chassis ID`	Chassis ID that uniquely identifies the neighbor.
`Neighbor Port Name`	Port ID of the neighbor.
`Neighbor Sys Name`	System name of the LLDP neighbor.
`Neighbor Capability`	Capabilities that are supported and enabled on the neighbor.
`System Capability`	System Capabilities of the LLDP neighbor.
`MED Device Type`	LLDP-MED Device class (Class I, II, III or Network Connectivity)
`MED Power Source`	LLDP-MED Power Source

Related commands show lldp neighbors detail

show lldp neighbors detail

Overview This command displays in detail the information received from neighbors via specified ports. If no port list is supplied, detailed neighbor information for all ports is displayed.

Syntax

```
show lldp neighbors detail [base] [dot1] [dot3] [med] [interface
<port-list>]
```

Parameter	Description
`base`	Information for base TLVs.
`dot1`	Information for 802.1 TLVs.
`dot3`	Information for 803.1 TLVs.
`med`	Information for LLDP-MED TLVs.
<port-list>	The ports for which the neighbor information is to be shown.

Mode User Exec and Privileged Exec

Examples To display detailed neighbor information received via all ports, use the command:

```
awplus# show lldp neighbors detail
```

To display detailed neighbor information received via ports 1.0.1, use the command:

```
awplus# show lldp neighbors detail interface port1.0.1
```

Output Figure 62-5: Example output from the **show lldp neighbors detail** command

```
awplus#show lldp neighbors detail interface port1.0.1
LLDP Detailed Neighbor Information:

Local port1.0.1:
  Neighbors table last updated 0 hrs 0 mins 40 secs ago
  Chassis ID Type ................... MAC address
  Chassis ID ........................ 0004.cd28.8754
  Port ID Type ...................... Interface alias
  Port ID ........................... port1.0.6
  TTL ............................... 120 (secs)
  Port Description .................. [zero length]
  System Name ....................... awplus
  System Description ................ Allied Telesis router/switch, AW+ v5.4.6
  System Capabilities - Supported .. Bridge, Router
                      - Enabled .... Bridge, Router
  Management Addresses .............. 0004.cd28.8754
  Port VLAN ID (PVID) ............... 1
  Port & Protocol VLAN - Supported . Yes
                       - Enabled ... Yes
                       - VIDs ...... 5
  VLAN Names ........................ default, vlan5
  Protocol IDs ...................... 9000, 0026424203000000, 888e01, 8100,
                                      88090101, 00540000e302, 0800, 0806, 86dd
  MAC/PHY Auto-negotiation ......... Supported, Enabled
       Advertised Capability ....... 1000BaseTFD, 100BaseTXFD, 100BaseTX,
                                     10BaseTFD, 10BaseT
       Operational MAU Type ........ 1000BaseTFD (30)
  Power Via MDI (PoE) ............... [not advertised]
  Link Aggregation .................. Supported, Disabled
  Maximum Frame Size ................ 1522 (Octets)
  LLDP-MED Device Type .............. Network Connectivity
  LLDP-MED Capabilities ............. LLDP-MED Capabilities, Network Policy,
                                      Location Identification,
                                      Extended Power - PSE, Inventory
  Network Policy .................... [not advertised]
  Location Identification .......... [not advertised]
  Extended Power Via MDI (PoE) ..... PD
           Power Source ............. PSE
           Power Priority .......... High
           Power Value ............. 4.4 Watts
  Inventory Management:
           Hardware Revision ....... X1-0
           Firmware Revision ....... 1.1.0
           Software Revision ....... v5.4.6
           Serial Number ........... M1NB73008
           Manufacturer Name ....... Allied Telesis Inc.
           Model Name .............. x230-28GP
           Asset ID ................ [zero length]
```

Table 64: Parameters in the output of the **show lldp neighbors detail** command

Parameter	Description
`Chassis ID Type`	Type of the Chassis ID.
`Chassis ID`	Chassis ID that uniquely identifies the neighbor.
`Port ID Type`	Type of the Port ID.
`Port ID`	Port ID of the neighbor.
`TTL`	Number of seconds that the information advertised by the neighbor remains valid.
`Port Description`	Port description of the neighbor's port.
`System Name`	Neighbor's system name.
`System Description`	Neighbor's system description.
`System Capabilities (Supported)`	Capabilities that the neighbor supports.
`System Capabilities (Enabled)`	Capabilities that are enabled on the neighbor.
`Management Addresses`	List of neighbor's management addresses.
`Port VLAN ID (PVID)`	VLAN identifier associated with untagged or priority tagged frames for the neighbor port.
`Port & Protocol VLAN (Supported)`	Whether Port & Protocol VLAN is supported on the LLDP neighbor.
`Port & Protocol VLAN (Enabled)`	Whether Port & Protocol VLAN is enabled on the LLDP neighbor.
`Port & Protocol VLAN (VIDs)`	List of Port & Protocol VLAN identifiers.
`VLAN Names`	List of names of VLANs that the neighbor's port belongs to.
`Protocol IDs`	List of protocols that are accessible through the neighbor's port.
`MAC/PHY Auto-negotiation`	Auto-negotiation configuration and status
`Power Via MDI (PoE)`	PoE configuration and status of 802.3 Power-Via-MDI TLV
`Link Aggregation`	Link aggregation information

Table 64: Parameters in the output of the **show lldp neighbors detail** command (cont.)

Parameter	Description
`Maximum Frame Size`	The maximum frame size capability
`LLDP-MED Device Type`	LLDP-MED Device type
`LLDP-MED Capabilities`	LLDP-MED capabilities supported
`Network Policy`	List of network policies
`Location Identification`	Location information
`Extended Power Via MDI (PoE)`	PoE-capability and current status
`Inventory Management`	Inventory information

Related commands show lldp neighbors

show lldp statistics

Overview This command displays the global LLDP statistics (packet and event counters).

Syntax

```
show lldp statistics
```

Mode User Exec and Privileged Exec

Example To display global LLDP statistics information, use the command:

```
awplus# show lldp statistics
```

Output

Table 65: Example output from the **show lldp statistics** command

```
awplus# show lldp statistics

Global LLDP Packet and Event counters:

  Frames:    Out ................... 345
             In .................... 423
             In Errored ............ 0
             In Dropped ............ 0
  TLVs:      Unrecognized .......... 0
             Discarded ............. 0
  Neighbors: New Entries ........... 20
             Deleted Entries ....... 20
             Dropped Entries ....... 0
             Entry Age-outs ........ 20
```

Table 66: Parameters in the output of the **show lldp statistics** command

Parameter	Description
Frames Out	Number of LLDPDU frames transmitted.
Frames In	Number of LLDPDU frames received.
Frames In Errored	Number of invalid LLDPDU frames received.
Frames In Dropped	Number of LLDPDU frames received and discarded for any reason.
TLVs Unrecognized	Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types.
TLVs Discarded	Number of LLDP TLVs discarded for any reason.
Neighbors New Entries	Number of times the information advertised by neighbors has been inserted into the neighbor table.

Table 66: Parameters in the output of the **show lldp statistics** command (cont.)

Parameter	Description
`Neighbors Deleted Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table.
`Neighbors Dropped Entries`	Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.
`Neighbors Entry Age-outs Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired.

Related commands

clear lldp statistics

show lldp statistics interface

show lldp statistics interface

Overview This command displays the LLDP statistics (packet and event counters) for specified ports. If no port list is supplied, LLDP statistics for all ports are displayed.

Syntax

```
show lldp statistics interface [<port-list>]
```

Parameter	Description
<port-list>	The ports for which the statistics are to be shown.

Mode User Exec and Privileged Exec

Examples To display LLDP statistics information for all ports, use the command:

```
awplus# show lldp statistics interface
```

To display LLDP statistics information for ports 1.0.1 and 1.0.6, use the command:

```
awplus# show lldp statistics interface port1.0.1,port1.0.6
```

Output

Table 67: Example output from the **show lldp statistics interface** command

```
awplus# show lldp statistics interface port1.0.1,port1.0.6

LLDP Packet and Event Counters:

port1.0.1
  Frames:    Out ................... 27
             In .................... 22
             In Errored ............ 0
             In Dropped ............ 0
  TLVs:      Unrecognized .......... 0
             Discarded ............. 0
  Neighbors: New Entries ........... 3
             Deleted Entries ....... 0
             Dropped Entries ....... 0
             Entry Age-outs ........ 0

port1.0.6
  Frames:    Out ................... 15
             In .................... 18
             In Errored ............ 0
             In Dropped ............ 0
  TLVs:      Unrecognized .......... 0
             Discarded ............. 0
  Neighbors: New Entries ........... 1
             Deleted Entries ....... 0
             Dropped Entries ....... 0
             Entry Age-outs ........ 0
```

Table 68: Parameters in the output of the **show lldp statistics interface** command

Parameter	Description
`Frames Out`	Number of LLDPDU frames transmitted.
`Frames In`	Number of LLDPDU frames received.
`Frames In Errored`	Number of invalid LLDPDU frames received.
`Frames In Dropped`	Number of LLDPDU frames received and discarded for any reason.
`TLVs Unrecognized`	Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types.
`TLVs Discarded`	Number of LLDP TLVs discarded for any reason.
`Neighbors New Entries`	Number of times the information advertised by neighbors has been inserted into the neighbor table.
`Neighbors Deleted Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table.
`Neighbors Dropped Entries`	Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.
`Neighbors Entry Age-outs Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired.

Related commands

clear lldp statistics

show lldp statistics

show location

Overview Use this command to display selected location information configured on the switch.

Syntax

```
show location {civic-location|coord-location|elin-location}
```

```
show location {civic-location|coord-location|elin-location}
identifier {<civic-loc-id>|<coord-loc-id>|<elin-loc-id>}
```

```
show location {civic-location|coord-location|elin-location}
interface <port-list>
```

Parameter	Description
`civic-location`	Display civic location information.
`coord-location`	Display coordinate location information.
`elin-location`	Display ELIN (Emergency Location Identifier Number) information.
<civic-loc-id>	Civic address location identifier, in the range 1 to 4095.
<coord-loc-id>	Coordinate location identifier, in the range 1 to 4095.
<elin-loc-id>	ELIN location identifier, in the range 1 to 4095.
<port-list>	Ports to display information about.

Mode User Exec and Privileged Exec

Examples To display a civic address location configured on port1.0.1, use the command:

```
awplus# show location civic-location interface port1.0.1
```

Table 69: Example output from the **show location** command

```
awplus# show location civic-location interface port1.0.1
Port     ID   Element Type          Element Value
-------------------------------------------------------------
1.0.1    1    Country               NZ
              City                  Christchurch
              Street-suffix         Avenue
              House-number          27
              Primary-road-name     Nazareth
```

To display coordinate location information configured on the identifier 1, use the command:

```
awplus# show location coord-location identifier 1
```

Table 70: Example output from the **show location** command

```
awplus# show location coord-location identifier 1
  ID  Element Type             Element Value
------------------------------------------------------------------
  1   Latitude Resolution      15 bits
      Latitude                 38.898648113012313842773437 5 degrees
      Longitude Resolution     15 bits
      Longitude                130.232323229312896728515625 0 degrees
      Altitude Resolution      10 bits
      Altitude                 2.50000000 meters
      Map Datum                WGS 84
```

The coordinate location information displayed may differ from the information entered because it is stored in binary format. For more information, see the location coord-location configuration command.

To display all ELIN location information configured on the switch, use the command:

```
awplus# show location elin-location
```

Table 71: Example output from the **show location elin-location** command

```
awplus# show location elin-location
  ID  ELIN
-----------------------------------
  1   1234567890
  2   5432154321
```

Related commands

location elin-location-id

location civic-location identifier

location civic-location configuration

location coord-location identifier

location coord-location configuration

location elin-location

Command changes

Version 5.4.8-2.1: Command added to AR2050V, AR3050S, AR4050S

63 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 3148
- "delete mail" on page 3149
- "mail" on page 3150
- "mail from" on page 3152
- "mail smtpserver" on page 3153
- "mail smtpserver authentication" on page 3154
- "mail smtpserver port" on page 3156
- "show counter mail" on page 3158
- "show mail" on page 3159
- "undebug mail" on page 3160

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 63-1: 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 25.

Syntax

```
mail smtpserver port <port>
no mail smtpserver port
```

Parameter	Description
<port>	Port number from the range 1 to 65535

Default Port 25 is the default port.

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 remove the configured port and set it back to the default port 25, use the commands:

```
awplus# configure terminal
awplus(config)# no mail smtpserver port
```

Output Figure 63-2: 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
Debug                                : Disabled

awplus#show running-config
!
mail smtpserver port 587
!
```

Related commands

debug mail

delete mail

mail

mail from

mail smtpserver

mail smtpserver authentication

show counter mail

show mail

Command changes Version 5.4.8-1.1: 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 63-3: 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 63-4: Example output from the **show mail** command:

```
awplus#show mail
Mail Settings
-------------------------------------------------------------
State                                : Alive
SMTP Server                          : example.net
Host Name                            : test@example.com
Debug                                : Enabled

Messages
-------------------------------------------------------------
To                                   : rei@nerv.com
Subject                              : The WAN is down
Message-ID                           : 20180615121150.8663

To                                   : rei@nerv.com
Subject                              : WAN is not connecting in lab
Message-ID                           : 20180614142502.19308

To                                   : rei@nerv.com
Subject                              : The LAN is not functioning
Message-ID                           : 20180614141911.29709
```

Related commands

delete mail

mail

mail from

mail smtpserver

show counter mail

undebug mail

undebug mail

Overview This command applies the functionality of the no debug mail command.

64 RMON Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure Remote Monitoring (RMON).

For an introduction to RMON and an RMON configuration example, see the RMON Feature Overview and Configuration Guide.

RMON is disabled by default in AlliedWare Plus™. No RMON alarms or events are configured.

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

Command List

- "rmon alarm" on page 3162
- "rmon collection history" on page 3165
- "rmon collection stats" on page 3166
- "rmon event" on page 3167
- "show rmon alarm" on page 3168
- "show rmon event" on page 3169
- "show rmon history" on page 3171
- "show rmon statistics" on page 3173

rmon alarm

Overview Use this command to configure an RMON alarm to monitor the value of an SNMP object, and to trigger specified events when the monitored object crosses specified thresholds.

To specify the action taken when the alarm is triggered, use the event index of an event defined by the rmon event command.

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

NOTE: *Only alarms for switch port interfaces, not for VLAN interfaces, can be configured.*

Syntax

```
rmon alarm <alarm-index> <oid> interval <1-2147483647>
{delta|absolute} rising-threshold <1-2147483647> event
<rising-event-index> falling-threshold <1-2147483647> event
<falling-event-index> alarmstartup [1|2|3] [owner <owner>]
```

```
rmon alarm <alarm-index> <oid> interval <1-4294967295>
{delta|absolute} rising-threshold <1-2147483647> event
eventwatch falling-threshold <1-2147483647> event eventwatch
[owner <owner>]
```

```
no rmon alarm <alarm-index>
```

Parameter	Description
<alarm-index>	*<1-65535>* Alarm entry index value.
<oid>	The variable SNMP MIB Object Identifier (OID) name to be monitored, in the format etherStatsEntry.*<field>*.*<stats-index>*. For example, etherStatsEntry.5.22 is the OID for the etherStatsPkts field in the etherStatsEntry table for the interface defined by the *<stats-index>* 22 in the rmon collection stats command.
interval *<1-2147483647>*	Polling interval in seconds.
delta	The RMON MIB alarmSampleType: the change in the monitored MIB object value between the beginning and end of the polling interval.
absolute	The RMON MIB alarmSampleType: the value of the monitored MIB object.
rising-threshold *<1-2147483647>*	Rising threshold value of the alarm entry in seconds.
<rising-event-index>	*<1-65535>* The event to be triggered when the monitored object value reaches the rising threshold value. This is an event index of an event specified by the rmon event command.

Parameter	Description
`eventwatch`	The alarm triggers an eventwatch event. This mechanism is used by Vista Manager EX, the Allied Telesis network management and monitoring tool. Do not use this parameter; use the *<rising-event-index>* parameter instead.
`falling-threshold <1-2147483647>`	Falling threshold value of the alarm entry in seconds.
<falling-event-index>	*<1-65535>* The event to be triggered when the monitored object value reaches the falling threshold value. This is an event index of an event specified by the rmon event command.
`eventwatch`	The alarm triggers an eventwatch event. This mechanism is used by Vista Manager EX, the Allied Telesis network management and monitoring tool. Do not use this parameter; use the *<rising-event-index>* parameter instead.
`alarmstartup {1|2|3}`	Whether RMON can trigger a falling alarm (1), a rising alarm (2) or either (3) when you first start monitoring. See the Usage section for more information. The default is setting 3 (either).
`owner <owner>`	Arbitrary owner name to identify the alarm entry.

Default By default, there are no alarms.

Mode Global Configuration

Usage notes RMON alarms have a rising and falling threshold. Once the alarm monitoring is operating, you cannot have a falling alarm unless there has been a rising alarm and vice versa.

However, when you start RMON alarm monitoring, an alarm must be generated without the other type of alarm having first been triggered. The **alarmstartup** parameter allows this. It is used to say whether RMON can generate a rising alarm (1), a falling alarm (2) or either alarm (3) as the first alarm.

Note that the SNMP MIB Object Identifier (OID) indicated in the command syntax with *<oid>* must be specified as a dotted decimal value with the form etherStatsEntry.*<field>*.*<stats-index>*, for example, etherStatsEntry.22.5.

Example To configure an alarm to monitor the change per minute in the etherStatsPkt value for interface 22 (defined by stats-index 22 in the rmon collection stats command), to trigger event 2 (defined by the rmon event command) when it reaches the rising threshold 400, and to trigger event 3 when it reaches the falling threshold 200, and identify this alarm as belonging to Maria, use the commands:

```
awplus# configure terminal

awplus(config)# rmon alarm 229 etherStatsEntry.22.5 interval 60
delta rising-threshold 400 event 2 falling-threshold 200 event
3 alarmstartup 3 owner maria
```

Related commands

rmon collection stats

rmon event

rmon collection history

Overview Use this command to create a history statistics control group to store a specified number of snapshots (buckets) of the standard RMON statistics for the switch port, and to collect these statistics at specified intervals. If there is sufficient memory available, then the device will allocate memory for storing the set of buckets that comprise this history control.

Use the **no** variant of this command to remove the specified history control configuration.

NOTE: *Only a history for switch port interfaces, not for VLAN interfaces, can be collected.*

Syntax

```
rmon collection history <history-index> [buckets <1-65535>]
[interval <1-3600>] [owner <owner>]
```

```
no rmon collection history <history-index>
```

Parameter	Description
`<history-index>`	*<1-65535>* A unique RMON history control entry index value.
`buckets <1-65535>`	Number of requested buckets to store snapshots. Default 50 buckets.
`interval <1-3600>`	Polling interval in seconds. Default 1800 second polling interval.
`owner <owner>`	Owner name to identify the entry.

Default The default interval is 1800 seconds and the default buckets is 50 buckets.

Mode Interface Configuration

Example To create a history statistics control group with ID 200 to store 500 snapshots with an interval of 600 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# rmon collection history 200 buckets 500
interval 600 owner herbert
```

To disable the history statistics control group, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no rmon collection history 200
```

rmon collection stats

Overview Use this command to enable the collection of RMON statistics on a switch port, and assign an index number by which to access these collected statistics.

Use the **no** variant of this command to stop collecting RMON statistics on this switch port.

NOTE: *Only statistics for switch port interfaces, not for VLAN interfaces, can be collected.*

Syntax

```
rmon collection stats <collection-index> [owner <owner>]
no rmon collection stats <collection-index>
```

Parameter	Description
<collection-index>	*<1-65535>* Give this collection of statistics an index number to uniquely identify it. This is the index to use to access the statistics collected for this switch port.
owner *<owner>*	An arbitrary owner name to identify this statistics collection entry.

Default RMON statistics are not enabled by default.

Mode Interface Configuration

Example To enable the collection of RMON statistics with a statistics index of 200, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# rmon collection stats 200 owner myrtle
```

To to stop collecting RMON statistics, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no rmon collection stats 200
```

rmon event

Overview Use this command to create an event definition for a log or a trap or both. Then you can use this event index in the rmon alarm command to indicate whether to send an SNMP trap or log message (or both) when an alarm is triggered.

Use the **no** variant of this command to remove the event definition.

Syntax

```
rmon event <event-index> [description <description>|owner
<owner>| trap <trap>]
```

```
rmon event <event-index> [log [description <description>|owner
<owner>|trap <trap>] ]
```

```
rmon event <event-index> [log trap [description
<description>|owner <owner>] ]
```

```
no rmon event <event-index>
```

Parameter	Description
<event-index>	*<1-65535>* Unique event entry index value.
log	Log event type.
trap	Trap event type.
log trap	Log and trap event type.
description*<description>*	Event entry description.
owner *<owner>*	Owner name to identify the entry.

Default No event is configured by default.

Mode Global Configuration

Example To create an event definition with an index of 299 for a log, use this command:

```
awplus# configure terminal
awplus(config)# rmon event 299 log description cond3 owner
alfred
```

To remove the event definition, use the command:

```
awplus# configure terminal
awplus(config)# no rmon event 299
```

Related commands rmon alarm

show rmon alarm

Overview Use this command to display the alarms and threshold configured for the RMON probe.

NOTE: *Only the alarms for switch port interfaces, not for VLAN interfaces, can be shown.*

Syntax

```
show rmon alarm
```

Mode User Exec and Privileged Exec

Example To display the alarms and threshold, use this command:

```
awplus# show rmon alarm
```

Related commands rmon alarm

show rmon event

Overview Use this command to display the events configured for the RMON probe.

NOTE: *Only the events for switch port interfaces, not for VLAN interfaces, can be shown.*

Syntax

```
show rmon event
```

Mode User Exec and Privileged Exec

Output Figure 64-1: Example output from the **show rmon event** command

```
awplus#sh rmon event
 event Index = 787
       Description TRAP
        Event type log & trap
         Event community name gopher
       Last Time Sent = 0
       Owner  RMON_SNMP

 event Index = 990
       Description TRAP
        Event type trap
         Event community name teabo
       Last Time Sent = 0
       Owner  RMON_SNMP
```

NOTE: *The following etherStats counters are not currently available for Layer 3 interfaces:*

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

Example To display the events configured for the RMON probe, use this command:

```
awplus# show rmon event
```

Related commands rmon event

show rmon history

Overview Use this command to display the parameters specified on all the currently defined RMON history collections on the device.

NOTE: *Only the history for switch port interfaces, not for VLAN interfaces, can be shown.*

Syntax

```
show rmon history
```

Mode User Exec and Privileged Exec

Output Figure 64-2: Example output from the **show rmon history** command

```
awplus#sh rmon history
 history index = 56
         data source ifindex = 4501
         buckets requested = 34
        buckets granted = 34
        Interval = 2000
        Owner Andrew

 history index = 458
         data source ifindex = 5004
         buckets requested = 400
        buckets granted = 400
        Interval = 1500
        Owner trev
=========================================================
```

NOTE: *The following etherStats counters are not currently available for Layer 3 interfaces:*

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets

- etherStatsPkts1024to1518Octets

Example To display the parameters specified on all the currently defined RMON history collections, us the commands:

```
awplus# show rmon history
```

Related commands rmon collection history

show rmon statistics

Overview Use this command to display the current values of the statistics for all the RMON statistics collections currently defined on the device.

NOTE: *Only statistics for switch port interfaces, not for VLAN interfaces, can be shown.*

Syntax

```
show rmon statistics
```

Mode User Exec and Privileged Exec

Example To display the current values of the statistics for all the RMON statistics collections, us the commands:

```
awplus# show rmon statistics
```

Output Figure 64-3: Example output from the **show rmon statistics** command

```
awplus#show rmon statistics
    rmon collection index 45
    stats->ifindex = 4501
    input packets 1279340, bytes 85858960, dropped 00, multicast packets 1272100
    output packets 7306090, bytes 268724, multicast packets 7305660 broadcast
packets 290
    rmon collection index 679
    stats->ifindex = 5013
    input packets 00, bytes 00, dropped 00, multicast packets 00
    output packets 8554550, bytes 26777324, multicast packets 8546690 broadcast
packets 7720
```

NOTE: *The following etherStats counters are not currently available for Layer 3 interfaces:*

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets

- etherStatsPkts1024to1518Octets

Related commands rmon collection stats

65 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 3177
- "clear ssh" on page 3178
- "crypto key destroy hostkey" on page 3179
- "crypto key destroy userkey" on page 3180
- "crypto key generate hostkey" on page 3181
- "crypto key generate userkey" on page 3183
- "crypto key pubkey-chain knownhosts" on page 3184
- "crypto key pubkey-chain userkey" on page 3186
- "debug ssh client" on page 3188
- "debug ssh server" on page 3189
- "service ssh" on page 3190
- "show banner login" on page 3192
- "show crypto key hostkey" on page 3193
- "show crypto key pubkey-chain knownhosts" on page 3195
- "show crypto key pubkey-chain userkey" on page 3196
- "show crypto key userkey" on page 3197
- "show running-config ssh" on page 3198
- "show ssh" on page 3200
- "show ssh client" on page 3202

- "show ssh server" on page 3203
- "show ssh server allow-users" on page 3205
- "show ssh server deny-users" on page 3206
- "ssh" on page 3207
- "ssh client" on page 3210
- "ssh server" on page 3212
- "ssh server allow-users" on page 3214
- "ssh server authentication" on page 3216
- "ssh server deny-users" on page 3218
- "ssh server max-auth-tries" on page 3220
- "ssh server resolve-host" on page 3221
- "ssh server scp" on page 3222
- "ssh server secure-ciphers" on page 3223
- "ssh server secure-kex" on page 3224
- "ssh server sftp" on page 3226
- "undebug ssh client" on page 3227
- "undebug ssh server" on page 3228

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.

When you enable the SSH server, the server automatically generates an SSHv2 host key pair (public and private keys), using RSA with 1024-bit key generation (except for switches in secure mode, which use ECDSA with a curve length of 384). 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.

Syntax

```
crypto key destroy hostkey {dsa|ecdsa|rsa|rsa1}
```

Parameters	Description
dsa	Deletes the existing DSA public and private keys.
ecdsa	Deletes the existing ECDSA public and private keys.
rsa	Deletes the existing RSA public and private keys configured for SSH version 2 connections.
rsa1	Deletes the existing RSA public and private keys configured for SSH version 1 connections.

Mode Global Configuration

Example To destroy the RSA host key used for SSH version 2 connections, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy hostkey rsa
```

Related commands

crypto key generate hostkey

service ssh

crypto key destroy userkey

Overview This command destroys the existing public and private keys of an SSH user configured on the device.

Syntax

```
crypto key destroy userkey <username> {dsa|rsa|rsa1}
```

Parameters	Description
`<username>`	Name of the user whose userkey you are destroying. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
`dsa`	Deletes the existing DSA userkey.
`rsa`	Deletes the existing RSA userkey configured for SSH version 2 connections.
`rsa1`	Deletes the existing RSA userkey for SSH version 1 connections.

Mode Global Configuration

Example To destroy the RSA user key for the SSH user `remoteuser`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy userkey remoteuser rsa
```

Related commands

crypto key generate hostkey

show ssh

show crypto key hostkey

crypto key generate hostkey

Overview This command generates public and private keys for the SSH server.

When you enable the SSH server, the server automatically generates an SSHv2 host key pair (public and private keys), using RSA with 1024-bit key generation (except for switches in secure mode, which use ECDSA with a curve length of 384).

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.

In secure mode, only ECDSA host keys are allowed.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

Syntax

```
crypto key generate hostkey {dsa} [<768-1024>]
crypto key generate hostkey {rsa|rsa1} [<768-32768>]
crypto key generate hostkey {ecdsa} [<256|384>]
```

Parameters	Description
`dsa`	Creates a DSA hostkey. Both SSH version 1 and 2 connections can use the DSA hostkey.
`rsa`	Creates an RSA hostkey for SSH version 2 connections.
`rsa1`	Creates an RSA hostkey for SSH version 1 connections.
`ecdsa`	Creates an ECDSA hostkey. Both SSH version 1 and 2 connections can use the ECDSA hostkey.
<768-32768>	The length in bits of the generated key. The default is 1024 bits.
<256|384>	The ECDSA key size in bits. The default is 256, but it can be set to 384.

Default The default key length for RSA and DSA is 1024 bits.

The default key size for ECDSA is 256 bits.

Mode Global Configuration

Examples To generate an RSA host key for SSH version 2 connections that is 2048 bits in length, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa 2048
```

To generate a DSA host key, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate dsa
```

To generate an ECDSA host key with an elliptic curve size of 384 bits, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate ecdsa 384
```

Related commands

crypto key destroy hostkey

service ssh

show crypto key hostkey

crypto key generate userkey

Overview This command generates public and private keys for an SSH user using either an RSA or DSA cryptography algorithm. To use public key authentication, copy the public key of the user onto the remote SSH server.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

Syntax

```
crypto key generate userkey <username> {dsa} [<768-1024>]
crypto key generate userkey <username> {rsa|rsa1} [<768-32768>]
crypto key generate userkey <username> {ecdsa} [<256|384>]
```

Parameters	Description
<username>	Name of the user that the user key is generated for. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
dsa	Creates a DSA userkey. Both SSH version 1 and 2 connections can use a key created with this command.
rsa	Creates an RSA userkey for SSH version 2 connections.
rsa1	Creates an RSA userkey for SSH version 1 connections.
ecdsa	Creates an ECDSA hostkey. Both SSH version 1 and 2 connections can use the ECDSA hostkey.
<768-32768>	The length in bits of the generated key. The default is 1024 bits.
<256|384>	The ECDSA key size in bits. The default is 256, but it can be set to 384.

Mode Global Configuration

Examples To generate a 2048-bits RSA user key for SSH version 2 connections for the user "bob", use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey bob rsa 2048
```

To generate a DSA user key for the user "lapo", use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey lapo dsa
```

Related commands crypto key pubkey-chain userkey

show crypto key userkey

crypto key pubkey-chain knownhosts

Overview This command adds a public key of the specified SSH server to the known host database on your device. The SSH client on your device uses this public key to verify the remote SSH server.

The key is retrieved from the server. Before adding a key to this database, check that the key sent to you is correct.

If the server's key changes, or if your SSH client does not have the public key of the remote SSH server, then your SSH client will inform you that the public key of the server is unknown or altered.

The **no** variant of this command deletes the public key of the specified SSH server from the known host database on your device.

Syntax

```
crypto key pubkey-chain knownhosts [ip|ipv6] <hostname>
[rsa|dsa|rsa1]
no crypto key pubkey-chain knownhosts <1-65535>
```

Parameter	Description
`ip`	Keyword used prior to specifying an IPv4 address
`ipv6`	Keyword used prior to specifying an IPv6 address
<hostname>	IPv4/IPv6 address or hostname of a remote server in the format `a.b.c.d` for an IPv4 address, or in the format `x:x::x:x` for an IPv6 address.
`rsa`	Specify the RSA public key of the server to be added to the known host database.
`dsa`	Specify the DSA public key of the server to be added to the known host database.
`rsa1`	Specify the SSHv1 public key of the server to be added to the know host database.
<1-65535>	Specify a key identifier when removing a key using the **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

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, the server automatically generates an SSHv2 host key pair (public and private keys), using RSA with 1024-bit key generation (except for switches in Secure Mode, which use ECDSA with a curve length of 384). 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 disables the Secure Shell server. When the Secure Shell server is disabled, connections from SSH, SCP, and SFTP clients are not accepted. This command does not affect existing SSH sessions. To terminate existing sessions, use the clear ssh command.

Syntax

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

Default The Secure Shell server is disabled by default. Both IPv4 and IPv6 Secure Shell server are enabled when you issue **service ssh** without specifying the optional **ip** or **ipv6** parameters.

By default, the server supports both SSH version 2 and SSH version 1, except when in Secure Mode (see the crypto secure-mode command). SSH version 1 is not available in Secure Mode.

Mode Global Configuration

Examples To enable both the IPv4 and the IPv6 Secure Shell server, use the commands:

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

To enable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ip
```

To enable the IPv6 Secure Shell server only, use the commands:

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

To disable both the IPv4 and the IPv6 Secure Shell server, use the commands:

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

To disable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ip
```

To disable the IPv6 Secure Shell server only, use the commands:

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

Related commands

crypto key generate hostkey

show running-config ssh

show ssh server

ssh server allow-users

ssh server deny-users

show banner login

Overview This command displays the banner message configured on the device. The banner message is displayed to the remote user before user authentication starts.

Syntax

```
show banner login
```

Mode User Exec, Privileged Exec, Global Configuration, Interface Configuration, Line Configuration

Example To display the current login banner message, use the command:

```
awplus# show banner login
```

Related commands banner login (SSH)

show crypto key hostkey

Overview This command displays the public keys generated on the device for the SSH server.

When you enable the SSH server, the server automatically generates an SSHv2 host key pair (public and private keys), using RSA with 1024-bit key generation (except for switches in secure mode, which use ECDSA with a curve length of 384). 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.

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. Both SSH version 1 and 2 connections can use the DSA hostkey
ecdsa	Displays the ECDSA algorithm public key. Both SSH version 1 and 2 connections can use the ECDSA hostkey.
rsa	Displays the RSA algorithm public key for SSH version 2 connections.
rsa1	Displays the RSA algorithm public key for SSH version 1 connections.

Mode User Exec, Privileged Exec and Global Configuration

Examples To show the public keys generated on the device for SSH server, use the command:

```
awplus# show crypto key hostkey
```

To display the RSA public key of the SSH server, use the command:

```
awplus# show crypto key hostkey rsa
```

Output Figure 65-1: Example output from the **show crypto key hostkey** command

```
Type Bits   Fingerprint
-----------------------------------------------------------
rsa  2058   4e:7d:1d:00:75:79:c5:cb:c8:58:2e:f9:29:9c:1f:48
dsa  1024   fa:72:3d:78:35:14:cb:9a:1d:ca:1c:83:2c:7d:08:43
rsa1 1024   e2:1c:c8:8b:d8:6e:19:c8:f4:ec:00:a2:71:4e:85:8b
```

Table 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 65-2: 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

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 65-3: 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 65-4: 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 65-5: 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 65-6: 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 65-7: 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 "1", "2" or "2,1".
Connect Timeout	Time in seconds that the SSH client waits for an SSH session to establish. If the value is 0, the connection is terminated when it reaches the TCP timeout.
Debug	Whether debugging is active on the client.

Related commands show ssh server

show ssh server

Overview This command displays the current configuration of the Secure Shell server.

Note that changes to the SSH configuration affects only new SSH sessions coming from remote hosts, and does not affect existing sessions.

Syntax

```
show ssh server
```

Mode User Exec, Privileged Exec, and Global Configuration

Example To display the current configuration of the Secure Shell server, use the command:

```
awplus# show ssh server
```

Output Figure 65-8: Example output from the **show ssh server** command

```
Secure Shell Server Configuration
-----------------------------------------------------------------
SSH Server                          : Enabled
Port                                : 22
Version                             : 2
Services                            : scp, sftp
User Authentication                 : publickey, password
Resolve Hosts                       : Disabled
Session Timeout                     : 0 (Off)
Login Timeout                       : 60 seconds
Maximum Authentication Tries        : 6
Maximum Startups                    : 10
Debug                               : NONE
Ciphers                             : chacha20-poly1305@openssh.com,
aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm
@openssh.com
```

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 '1', '2' or '2,1'.
Services	List of the available Secure Shell service; one or more of SHELL, SCP or SFTP.
Authentication	List of available authentication methods.

Table 8: Parameters in the output of the **show ssh server** command (cont.)

Parameter	Description
`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`	The current ciphers in use.

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 65-9: 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 65-10: 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 {1|2}]
<remote-device> [<command>]
```

Syntax in secure mode

```
ssh [cipher {aes128-cbc|aes256-cbc}] [hmac {hmac-sha2-256}]
[public-key {ecdsa-sha2-nistp256|ecdsa-sha2-nistp384}] [key
exchange {ecdh-sha2-nistp256|ecdh-sha2-nistp384}] [ip|ipv6]
[user <username>|port <1-65535>|version {1|2}] <remote-device>
[<command>]
```

Parameter	Description
`cipher`	The supported cipher name. Select either: aes128-cbc or aes256-cbc.
`hmac`	The supported hmac name: hmac-sha2-256
`public-key`	The supported public-key name. Select either: ecdsa-sha2-nistp256 or ecdsa-sha2-nistp384
`key-exchange`	The supported key-exchange name. Select either: ecdsa-sha2-nistp256 or ecdsa-sha2-nistp384
`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.

Parameter	Description	
`version`	SSH client version. If version is specified, the SSH client supports only the specified SSH version. By default, SSH client uses SSHv2 first. If the server does not support SSHv2, it will try SSHv1. The default version can be configured by "ssh client" command.	
	`1`	Use SSH version 1.
	`2`	Use SSH 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

Usage notes This command contains some additional security parameters (cipher, hmac, public-key, and key exchange). To access these parameters you must enable Secure Mode on the device by using the command: **crypto secure-mode**.

```
awplus(config)# crypto secure-mode
```

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 with "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 secure-mode

crypto key pubkey-chain knownhosts

debug ssh client

ssh client

Command changes

Version 5.4.6-2.1: VRF-lite support added for AR-Series devices.

Version 5.4.8-1.2: secure mode syntax added for x220, x930, x550, XS900MX.

Version 5.4.8-2.1: secure mode syntax added for x950, SBx908 GEN2.

ssh client

Overview This command modifies the default configuration parameters of the Secure Shell (SSH) client. The configuration is used for any SSH client on the device to connect to remote SSH servers. Any parameters specified on SSH client explicitly override the default configuration parameters.

The change affects the current user shell only. When the user exits the login session, the configuration does not persist. This command does not affect existing SSH sessions.

The **no** variant of this command resets configuration parameters of the Secure Shell (SSH) client changed by the ssh client command, and restores the defaults.

This command does not affect the existing SSH sessions.

Syntax

```
ssh client {port <1-65535>|version {1|2}|session-timeout
<0-3600>|connect-timeout <1-600>}
```

```
no ssh client {port|version|session-timeout|connect-timeout}
```

Parameter	Description	
`port`	The default TCP port of the remote SSH server. If an SSH client specifies an explicit port of the server, it overrides the default TCP port. Default: 22	
	<1-65535>	TCP port number.
`version`	The SSH version used by the client for SSH sessions. The SSH client supports both version 2 and version 1 Default: version 2 Note: SSH version 2 is the default SSH version. SSH client supports SSH version 1 if SSH version 2 is not configured using a ssh version command.	
	`1`	SSH clients on the device supports SSH version 1 only.
	`2`	SSH clients on the device supports SSH version 2 only
`session-timeout`	The global session timeout for SSH sessions. If the session timer lapses since the last time an SSH client received data from the remote server, the session is terminated. If the value is 0, then the client does not terminate the session. Instead, the connection is terminated when it reaches the TCP timeout. Default: 0 (session timer remains off)	
	<0-3600>	Timeout in seconds.

Parameter	Description
`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

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.

By default, the server supports both SSH version 2 and SSH version 1, except when in Secure Mode (see the crypto secure-mode command). SSH version 1 is not available in Secure Mode.

Syntax

```
ssh server {[v1v2|v2only]|<1-65535>}
ssh server {[session-timeout <0-3600>] [login-timeout <1-600>]
[max-startups <1-128>]}
no ssh server {[session-timeout] [login-timeout]
[max-startups]}
```

Parameter	Description
`v1v2`	Supports both SSHv2 and SSHv1client connections. Default: v1v2
`v2only`	Supports SSHv2 client connections only.
<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).
	<0-3600> Timeout in seconds.
`login-timeout`	The maximum time period the server waits before disconnecting an unauthenticated client. Default: 60
	<1-600> Timeout in seconds.
`max-startups`	The maximum number of concurrent unauthenticated connections the server accepts. When the number of SSH connections awaiting authentication reaches the limit, the server drops any additional connections until authentication succeeds or the login timer expires for a connection. Default: 10
	<1-128> Number of sessions.

Mode Global Configuration

Examples To configure the session timer of SSH server to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 600
```

To configure the login timeout of SSH server to 30 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 30
```

To limit the number of SSH client connections waiting for authentication from SSH server to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-startups 3
```

To set max-startups parameters of SSH server to the default configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server max-startups
```

To support the Secure Shell server with TCP port 2200, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server 2200
```

To force the Secure Shell server to support SSHv2 only, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server v2only
```

To support both SSHv2 and SSHv1, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server v1v2
```

Related commands show ssh server

ssh client

ssh server allow-users

Overview This command adds a username pattern to the allow list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is accepted.

When there are no registered users in the server's database of allowed users, the SSH server does not accept SSH sessions even when enabled.

SSH server also maintains the deny list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

The **no** variant of this command deletes a username pattern from the allow list of the SSH server. To delete an entry from the allow list, the username and hostname pattern should match exactly with the existing entry.

Syntax

```
ssh server allow-users <username-pattern> [<hostname-pattern>]
no ssh server allow-users <username-pattern>
[<hostname-pattern>]
```

Parameter	Description
<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. Use the ip name-server command to add a DNS server to the list of servers that the device queries.

Example To resolve a host name using a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server resolve-hosts
```

Related commands

ip name-server

show ssh server

ssh server allow-users

ssh server deny-users

ssh server scp

Overview This command enables the Secure Copy (SCP) service on the SSH server. Once enabled, the server accepts SCP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SCP connections. The SCP service is enabled by default as soon as the SSH server is enabled.

The **no** variant of this command disables the SCP service on the SSH server. Once disabled, SCP requests from remote clients are rejected.

Syntax

```
ssh server scp
no ssh server scp
```

Mode Global Configuration

Examples To enable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server scp
```

To disable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server scp
```

Related commands show running-config ssh

show ssh server

ssh server secure-ciphers

Overview Use this command to set the SSH server to only negotiate ciphers regarded as current-best-practice.

Use the **no** variant of this command to return to the default setting of not set.

Syntax

```
ssh server secure-ciphers
no ssh server secure-ciphers
```

Parameter	Description
`secure-ciphers`	Negotiate only with ciphers that are still considered current-best-practice and secure

Default Not set

Mode Global Configuration

Usage notes This command uses the same cipher string as the OpenSSH default, which excludes CBC, as CBC has been regarded as a weak cipher.

When the command is used, the ciphers included are: chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com

Example To configure the SSH server to only negotiate ciphers regarded as current best practice, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-ciphers
```

Related commands show ssh server

Command changes Version 5.5.0-1.1: command added

ssh server secure-kex

Overview Use this command to specify only key exchange algorithms which are consistent with key exchange algorithms currently considered as best-current-practice to be used by the SSH server.

The algorithm list does not include diffie-hellman-group-exchange-sha1 key exchange algorithm.

Use the **no** variant of this command to disable the SSH server from using more secure key-exchange algorithms.

Syntax

```
ssh server secure-kex
no ssh server secure-kex
```

Parameter	Description
`secure-kex`	Use the best current practice secure key exchange (kex) list.

Default Disabled.

Mode Global Configuration

Example To enable the SSH server to use more secure key-exchange algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-kex
```

Output Figure 65-11: Example output from **show ssh server**

```
awplus#show ssh server
Secure Shell Server Cobfiguration
----------------------------------------------------------------
SSH Server                          : Disabled
Protocol                            : None
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                             : chacha20-poly1305@openssh.com,aes128-ctr,
                                       aes192-ctr,aes256-ctr,
                                       aes128-gcm@openssh.com,
                                       aes256-gcm@openssh.com
KEX                                 : curve25519-sha256@libssh.org,
                                        ecdh-sha2-nistp521,ecdh-sha2-nistp384,
                                        ecdh-sha2-nistp256,
                                        diffie-hellman-group-exchange-sha256
```

Related commands

ssh server

ssh server allow-users

ssh server authentication

ssh server deny-users

ssh server scp

ssh server sftp

ssh server max-auth-tries

ssh server secure-ciphers

Command changes Version 5.5.0-2.3: 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

undebug ssh client

Overview This command applies the functionality of the **no** debug ssh client command.

undebug ssh server

Overview This command applies the functionality of the **no** debug ssh server command.

66 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 3231
- "day" on page 3232
- "debug trigger" on page 3234
- "description (trigger)" on page 3235
- "repeat" on page 3236
- "script" on page 3237
- "show debugging trigger" on page 3239
- "show running-config trigger" on page 3240
- "show trigger" on page 3241
- "test" on page 3246
- "time (trigger)" on page 3247
- "trap" on page 3249
- "trigger" on page 3250
- "trigger activate" on page 3251
- "type atmf node" on page 3252
- "type cpu" on page 3255
- "type interface" on page 3256
- "type linkmon-probe" on page 3257

- "type log" on page 3259
- "type memory" on page 3260
- "type periodic" on page 3261
- "type ping-poll" on page 3262
- "type reboot" on page 3263
- "type time" on page 3264
- "type usb" on page 3265
- "undebug trigger" on page 3266

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 66-1: Example output from the **show debugging trigger** command

```
awplus#debug trigger
awplus#show debugging trigger
Trigger debugging status:
  Trigger debugging is on

awplus#no debug trigger
awplus#show debugging trigger
Trigger debugging status:
  Trigger debugging is off
```

Related commands debug trigger

show running-config trigger

Overview This command displays the current running configuration of the trigger utility.

Syntax

```
show running-config trigger
```

Mode Privileged Exec

Example To display the current configuration of the trigger utility, use the command:

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

Output Figure 66-2: Example output from the **show running-config trigger** command

```
 trigger 1
  type card in

type usb in
 trigger 2

type usb out
 !
```

Related commands show trigger

show trigger

Overview This command displays configuration and diagnostic information about the triggers configured on the device. Specify the **show trigger** command without any options to display a summary of the configuration of all triggers.

Syntax

```
show trigger [<1-250>|counter|full]
```

Parameter	Description
<1-250>	Displays detailed information about a specific trigger, identified by its trigger ID.
`counter`	Displays statistical information about all triggers.
`full`	Displays detailed information about all triggers.

Mode Privileged Exec

Example To get summary information about all triggers, use the following command:

```
awplus# show trigger
```

Table 66-1: 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 66-2: 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 66-2: 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 66-3: Example output from **show trigger** for a specific trigger

```
awplus#show trigger 1
Trigger Configuration Details
-------------------------------------------------------------
Trigger ..................... 1
Name ........................ display cpu usage when pass 80%
Type and details ............ CPU (80% up)
Days ........................ smtwtfs
Active ...................... Yes
Test ........................ No
Trap ........................ Yes
Repeat ...................... Continuous
Modified .................... Fri Feb 3 17:18:44 2017
Number of activations ....... 0
Last activation ............. not activated
Number of scripts ........... 1
1. shocpu.scp
2.
3.
4.
5.
-------------------------------------------------------------
```

To display detailed information about all triggers, use the command:

```
awplus# show trigger full
```

Table 66-3: 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 67: 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 67: 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 66-4: Example output from **show trigger counter**

```
awplus# show trigger counter
Trigger Module Counters
-------------------------------------------------------
Trigger activations                              4
Last trigger activated                          55
Time triggers activated today                    0
Periodic triggers activated today                0
Interface triggers activated today               1
CPU triggers activated today                     2
Memory triggers activated today                  1
Reboot triggers activated today                  0
Ping-poll triggers activated today               0
USB event triggers activated today               0
Stack master fail triggers activated today       0
Stack member triggers activated today            0
Stack link triggers activated today              0
ATMF node triggers activated today               0
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
```

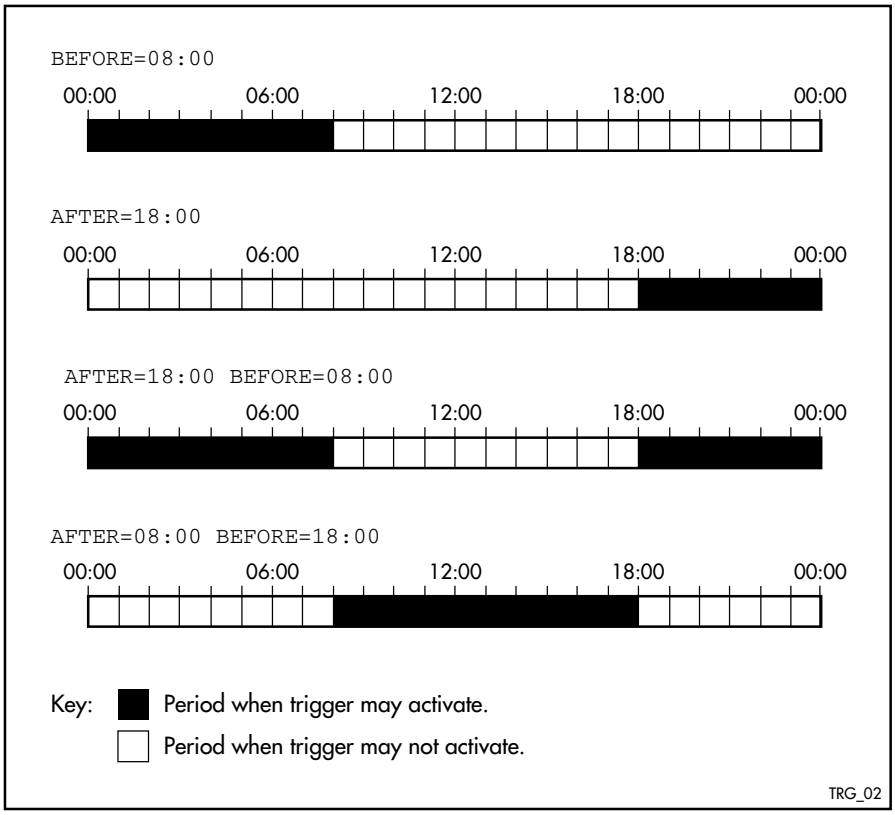
Related commands show trigger

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 node

Overview This command configures a trigger to be activated at an AMF node join event or leave event.

Syntax

```
type atmf node {join|leave}
```

Parameter	Description
join	AMF node join event.
leave	AMF node leave event.

Mode Trigger Configuration

CAUTION: Only configure this trigger on one device because it is a network wide event.

Example 1 To configure trigger 5 to activate at an AMF node leave event, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger) type atmf node leave
```

Example 2 The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
====================
node1, node2, node3:
====================

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=======
node1:
=======

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
001 Periodic (2 min)   Periodic Status Chk  Y  N  Y Continuous  1   smtwtfs
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------

==============
Node2, Node3,
==============

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------
```

Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
========
Node1:
========

trigger 1
 type periodic 2
 script 1 atmf.scp
trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!

============
Node2, Node3:
============

trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!
```

Related 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 port1.0.1 becomes operational, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 19
awplus(config-trigger)# type interface port1.0.1 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# trigger 1
awplus(config)# script 1 link-bad.scp
awplus(config)# 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# trigger 2
awplus(config)# script 1 link-good.scp
awplus(config)# 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

type usb

Overview Use this command to configure a trigger that activates on either the removal or the insertion of a USB storage device.

Syntax

```
type usb {in|out}
```

Parameter	Description
`in`	Trigger activates on insertion of a USB storage device.
`out`	Trigger activates on removal of a USB storage device.

Mode Trigger Configuration

Usage notes USB triggers cannot execute script files from a USB storage device.

Examples To configure trigger 1 to activate on the insertion of a USB storage device, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 1
awplus(config-trigger)# type usb in
```

Related commands

trigger

show running-config trigger

show trigger

undebug trigger

Overview This command applies the functionality of the **no** debug trigger command.

67 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 67-1: 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 3269
- "clear ping-poll" on page 3270
- "critical-interval" on page 3271
- "debug ping-poll" on page 3272

- "description (ping-polling)" on page 3273
- "fail-count" on page 3274
- "ip (ping-polling)" on page 3275
- "length (ping-poll data)" on page 3276
- "normal-interval" on page 3277
- "ping-poll" on page 3278
- "sample-size" on page 3279
- "show counter ping-poll" on page 3281
- "show ping-poll" on page 3283
- "source-ip" on page 3287
- "timeout (ping polling)" on page 3289
- "up-count" on page 3290
- "undebug ping-poll" on page 3291

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 67-1: 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 68: 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 67-2: 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 69: 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 69: 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 67-3: 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 70: 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 70: 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.

68 sFlow Commands

Introduction

Overview This chapter provides an alphabetical reference for sFlow commands.

For more information, see the sFlow Feature Overview and Configuration Guide.

Command List

- "debug sflow" on page 3293
- "debug sflow agent" on page 3294
- "sflow agent" on page 3295
- "sflow collector" on page 3297
- "sflow collector max-datagram-size" on page 3299
- "sflow enable" on page 3300
- "sflow max-header-size" on page 3301
- "sflow polling-interval" on page 3303
- "sflow sampling-rate" on page 3304
- "show debugging sflow" on page 3305
- "show running-config sflow" on page 3307
- "show sflow" on page 3308
- "show sflow interface" on page 3310
- "undebug sflow" on page 3311

debug sflow

Overview This command enables sFlow® debug message logging, for sFlow sampling and polling activity on the specified ports. If no ports are specified, sampling and/or polling debug messages are enabled for all ports.

The **no** variant of this command disables sFlow sampling and or polling debug message logging on the ports selected. If no ports are specified, sampling and/or polling debug messages are disabled on all ports.

Syntax

```
debug sflow [interface <port-list>] [sampling][polling]
no debug sflow [interface <port-list>] [sampling][polling]
```

Parameter	Description
`interface`	Interface information.
<port-list>	The ports for which sFlow debug is to be enabled. The ports to display information about. The port list can be: • a switch port (e.g. `port1.0.12`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.24` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.1-1.0.24`.
`sampling`	Debug sFlow sampling for the specified port(s).
`polling`	Debug sFlow polling for the specified port(s).

Default The sFlow sampling and or polling debug is disabled.

Mode Privileged Exec

Examples To enable sFlow debug message logging for polling and sampling on port1.0.1 and port1.0.7, use the commands:

```
awplus# debug sflow interface port1.0.1,port1.0.7 sampling
polling
```

To enable logging and polling of sFlow debug messages for polling and sampling on all ports, use the command:

```
awplus# debug sflow sampling polling
```

Related commands show debugging sflow

no debug all

debug sflow agent

Overview This command enables sFlow® debug message logging that is not specific to particular ports. For example, sending an sFlow datagram to the collector.

The **no** variant of this command applies the command default.

Syntax

```
debug sflow agent
no debug sflow agent
```

Default The sFlow agent debug message logging (that is not port specific) is disabled.

Mode Privileged Exec

Example To enable logging of sFlow agent debug messages, use the following command:

```
awplus# debug sflow agent
```

Related commands show debugging sflow

debug sflow

sflow agent

Overview This command sets the sFlow® agent IP address on the switch. This address is inserted into every sFlow datagram sent from the sFlow agent switch to the sFlow collector device. The sFlow collector can then uses this address to uniquely identify and to access the switch, such as for SNMP. We therefore recommend that you change this address as little as possible.

Although the agent address can be set to any valid IPv4 or IPv6 address; we recommended that you set the sFlow® agent IP address to be the **local address** that is configured on the switch. For information on local addresses and how to set them up, see the interface (to configure) command. This ensures that the sFlow collector can maintain connectivity to the switch irrespective of the addition or deletion of VLAN interfaces (each of which will have its own specific IP address). Note that sFlow is rendered inactive whenever the agent address is not set.

The **no** variant of this command applies its default setting to remove a configured address.

Syntax

```
sflow agent {ip <ip-address>|ipv6 <ipv6-address>}
no sflow agent {ip|ipv6}
```

Parameter	Description
<ip-address>	The IPv4 address of the switch that is acting as the sFlow agent.
<ipv6-address>	The IPv6 address of the switch that is acting as the sFlow agent. The IPv6 address uses the format X:X::X:X.

Default The sFlow agent address is unset.

Mode Global Configuration

Examples To set the sFlow agent (IPv4) address to `192.0.2.23`, use the command:

```
awplus# configure terminal
awplus(config)# sflow agent ip 192.0.2.23
```

To remove the sFlow agent (IPv4) address, use the command:

```
awplus# configure terminal
awplus(config)# no sflow agent ip
```

To set the sFlow agent (IPv6) address to `2001:0db8::1`, use the command:

```
awplus# configure terminal
awplus(config)# sflow agent ipv6 2001:0db8::1
```

To remove the sFlow agent (IPv6) address, use the command:

```
awplus# configure terminal
awplus(config)# no sflow agent ipv6
```

Related commands

show running-config sflow

show sflow

sflow collector

Overview This command sets the sFlow® agent's collector IP address and/or UDP port. This is the destination IP address and UDP port, for sFlow datagrams sent from the sFlow agent. The IP address can be any valid IPv4 or IPv6 address. Note that sFlow is rendered inactive whenever the collector address is set to 0.0.0.0 (for IPv4) or `::` (for IPv6).

The **no** variant of this command returns the IP address and UDP port values to their defaults, which will result in sFlow being deactivated.

Syntax

```
sflow collector {[ip <ip-address>|ipv6 <ipv6-address>]|[port <1-65535>]}
no sflow collector {[ip|ipv6]|[port]}
```

Parameter	Description
<ip-address>	IPv4 address of the remote sFlow collector.
<ipv6-address>	IPv6 address of remote sFlow collector. The IPv6 address uses the format X:X::X:X.
`port`	Destination UDP port for sFlow datagrams sent to the collector.
<1-65535>	UDP port number (default: 6343).

Default The collector address is `0.0.0.0` (which renders sFlow inactive), and the UDP port is `6343`.

Mode Global Configuration

Examples To set the sFlow collector address to `1920.2.25` and UDP port to `9000`, use the command:

```
awplus# configure terminal
awplus(config)# sflow collector ip 192.0.2.25 port 9000
```

To remove the sFlow collector IPv4 address and leave the UDP port unchanged, use the command:

```
awplus# configure terminal
awplus(config)# no sflow collector ip
```

To remove the sFlow collector IPv4 address and to remove the UDP port, use the command:

```
awplus# configure terminal
awplus(config)# no sflow collector ip port
```

To set the sFlow collector address to `2001:0db8::1` and leave the UDP port unchanged, use the command:

```
awplus# configure terminal
awplus(config)# sflow collector ipv6 2001:0db8::1
```

To remove the sFlow collector IPv6 address and leave the UDP port unchanged, use the command:

```
awplus# configure terminal
awplus(config)# no sflow collector ipv6
```

To remove the sFlow collector IPv6 address and to remove the UDP port, use the command:

```
awplus# configure terminal
awplus(config)# no sflow collector ipv6 port
```

Related commands

show running-config sflow

show sflow

sflow collector max-datagram-size

Overview This command sets the maximum size of the sFlow® datagrams sent to the collector.

The **no** variant of this command resets the maximum-datagram-size to the default.

Syntax

```
sflow collector max-datagram-size <200-1500>
no sflow collector max-datagram-size
```

Parameter	Description
<200-1500>	The maximum number of bytes that can be sent in an sFlow datagram sent from the agent to the collector.

Default 1400 bytes

Mode Global Configuration

Example To set the maximum datagram size to 1200, use the command:

```
awplus# configure terminal
awplus(config)# sflow collector max-datagram-size 1200
```

Related commands show running-config sflow

show sflow

sflow enable

Overview This command enables sFlow® globally on the switch.

The **no** variant of this command disables sFlow globally on the switch.

Note that enabling sFlow does not automatically set its operational status to active. To activate sFlow the following conditions need to be met:

- sFlow is enabled.
- The sFlow agent address is set.
- The sFlow collector address is set to a valid (non zero) IPv4 or IPv6 address.
- Polling or sampling is enabled on the ports to be sampled or polled.

Syntax

```
sflow enable
no sflow enable
```

Default sFlow is disabled globally on the switch.

Mode Global Configuration

Example To enable sFlow operation, use the command:

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

Related commands show running-config sflow

show sflow

sflow max-header-size

Overview This command sets the maximum header size of the Ethernet frames sampled on a specified port. The maximum header size is measured in bytes, referenced from the first byte of the Ethernet destination address and excludes the Ethernet FCS fields.

If a sampled Ethernet frame is longer than the maximum header size set by this command, then the frame will be truncated to the first N bytes before being placed in the sFlow datagram, where N is the maximum header size set by this command.

The **no** variant of this command resets the max-header-size to its default.

Syntax

```
sflow max-header-size <14-200>
no sflow max-header-size
```

Parameter	Description
<14-200>	The maximum number of header bytes to be sampled.

Default The max-header-size is 128 bytes.

Mode Interface Configuration

Usage notes The header size is measured from the first byte of the Ethernet frame MAC Destination Address.

- For an environment using standard TCP IPv4 over Ethernet frames, consider the following basic protocol structure:

  Ethernet header (including the 4 byte 802.1Q header component) = 18 bytes

  IPv4 header = 24 bytes

  TCP header = 24 bytes

  Total = 66 bytes

  CAUTION: *For IPv4, any data existing between 66 bytes and the value set by this command will be included in the sFlow packet samples. For example, with the default of 128 applied, up to 128-66=62 bytes of user data could be included in the sFlow datagram samples sent between the Agent and the Collector.*

  For more information, see the sFlow Feature Overview and Configuration Guide.

- A similar consideration can be made for an environment using TCP IPv6 over Ethernet:

  Ethernet header (including the 4 byte 802.1Q header component) = 18 bytes

  IPv6 header = 40 bytes

  TCP header = 24 bytes

  Total = 82 bytes

  CAUTION: *For IPv6, any data existing between 82 bytes and the value set by this command will be included in the sFlow packet samples. For example, with the default of 128 applied, up to 128-82=46 bytes of user data could be included in the sFlow datagram samples sent between the Agent and the Collector.*

Note that the agent-to-collector datagrams contain their own UDP headers, which are outside this calculation.

Example To set the maximum header size to 160 bytes for ports 1.0.1 and 1.0.7, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.7
awplus(config-if)# sflow max-header-size 160
```

Related commands

show running-config sflow

show sflow interface

sflow max-header-size

sflow polling-interval

Overview This command sets the sFlow® counter polling interval (in seconds) for the specified ports. A value of 0 disables polling. A counter sample is taken every N seconds where N is the value set by this command.

The **no** variant of this command applies the default.

Syntax

```
sflow polling-interval {0|<1-16777215>}
no sflow polling-interval
```

Parameter	Description
0	Disable polling (the default).
<1-16777215>	The polling interval in seconds.

Default The polling-interval is 0 (polling disabled).

Mode Interface Configuration

Example To set the polling interval to 60 seconds for ports 1.0.1 and 1.0.7, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.7
awplus(config-if)# sflow polling-interval 60
```

Related commands show running-config sflow

show sflow interface

sflow sampling-rate

Overview This command sets the mean sFlow® sampling rate for the specified ports. Sampling occurs every N frames (on average), where N is the rate value set via this command. The sampling rate applies to ingress and egress frames independently. For example, a value of 1000 will sample one frame in every 1000 frames received, i.e. one in every 1000 frames sent from the specified port. A value of 0 disables sampling on the specified port(s).

The **no** variant of this command applies the default.

Syntax

```
sflow sampling-rate <256-16777215>
no sflow sampling-rate
```

Parameter	Description
<256-16777215>	The sampling rate N, measured in Ethernet frames.

Default The sampling-rate is 0 (sampling disabled).

Mode Interface Configuration

Example To set the sampling rate to 500 for port1.0.1 and port1.0.3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.3
awplus(config-if)# sflow sampling-rate 500
```

Related commands show running-config sflow

show sflow interface

show debugging sflow

Overview This command displays sFlow® debug settings for agent operation, and for sampling and polling on specific interface ports. If no interface ports are specified, sampling and polling will be applied to all ports.

Syntax

```
show debugging sflow [interface <port-list>]
```

Parameter	Description
`interface`	The interface information.
`<port-list>`	The ports for which the sFlow debug settings are to be shown. The ports to display information about. The port list can be: • a switch port (e.g. `port1.0.6`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.6` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.3-1.0.6`.

Mode User Exec and Privileged Exec

Example To display sFlow debug settings on the agent, and for sampling and polling on ports 1.0.1 to 1.0.9, use the command:

```
awplus# show debugging sflow interface port1.0.1-1.0.9
```

Output Figure 68-1: Sample obtained for an sFlow agent

```
awplus# show debugging sflow interface port1.0.1-1.0.9

sFlow Agent Debug:    Enabled

          Sampling      Polling
Port       Debug         Debug
-------------------------------
1.0.1     Enabled       Enabled
1.0.2     Enabled          -
1.0.3        -             -
1.0.4        -             -
1.0.5        -             -
1.0.6        -          Enabled
1.0.7        -             -
1.0.8        -          Enabled
1.0.9        -          Enabled
```

To display sFlow debug settings for all ports, use the command:

```
awplus# show debugging sflow
```

Related commands

show running-config sflow

show sflow interface

show running-config sflow

Overview This command displays the running system information specific to the sFlow feature.

Syntax

```
show running-config sflow
```

Mode Privileged Exec and Global Configuration

Example To display the sFlow running configuration information, use the command:

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

Output Figure 68-2: Example output from the **show running-config sflow** command

```
awplus#sh run sflow
!
sflow agent ip 192.0.2.33
sflow collector ip 192.0.2.65
sflow collector max-datagram-size 1200
sflow enable
!
interface port1.0.11-port1.0.22
 sflow sampling-rate 512
```

Related commands show running-config

show sflow

Overview This command displays non-port-specific sFlow agent configuration and operational status.

Syntax

```
show sflow
```

Mode Privileged Exec

Example To display sFlow configuration and operational status, use the command:

```
awplus# show sflow
```

Output

Table 1: Example output from the **show sflow** command

```
sFlow Agent Configuration:                    Default Values
  sFlow Admin Status ........ Disabled        [Disabled]
  sFlow Agent Address ....... [not set]       [not set]
  Collector Address ......... 0.0.0.0         [0.0.0.0]
  Collector UDP Port ........ 6343            [6343]
  Tx Max Datagram Size ...... 1200            [1400]

sFlow Agent Status:
  Polling/sampling/Tx ....... Inactive because:
                                - sFlow is disabled
                                - Agent Addr is not set
                                - Collector Addr is 0.0.0.0
                                - Polling & sampling disabled
                                  on all ports
```

Table 2: Parameters in the output of the **show sflow** command

Output Parameter	Description
sFlow Admin Status	Whether sFlow agent operation is administratively enabled.
sFlow Agent Address	The sFlow agent IPv4 or IPv6 address for the device. sFlow is rendered inactive whenever the agent address is not set.
Collector Address	The IPv4 or IPv6 collector address to which sFlow datagrams are sent. sFlow is rendered inactive whenever the collector address is set to 0.0.0.0 or 0:0::0.0.
Collector UDP Port	The UDP port on the collector to which sFlow datagrams are sent.

Table 2: Parameters in the output of the **show sflow** command (cont.)

Output Parameter	Description
`Tx Max Datagram Size`	The maximum size of the sFlow datagrams sent to the collector.
`Polling/sampling/ Tx`	Whether sFlow sampling and/or polling (and hence sFlow datagram transmission) are active. If inactive the reasons are listed.

Related commands

show running-config sflow

show sflow interface

show sflow interface

Overview This command displays sFlow agent sampling and polling configuration for all ports or a specified port.

Syntax

```
show sflow interface [<ifrange>]
```

Parameter	Description
<ifrange>	The interface range.

Mode Privileged Exec

Example To display the sFlow sampling and polling configuration for port port1.0.1, use the command:

```
awplus# show sflow interface port1.0.1
```

Output Figure 68-3: Example output from the **show sflow interface**command

```
awplus#show sflow interface

sFlow Port Configuration:
  Default Values:
    Sampling Rate ........... 0 pkts (= disabled)
    Max Sample Header Size .. 128 bytes
    Polling Interval ........ 0 secs (= disabled)

               Sampling     Max Header     Polling
                 Rate          Size        Interval
Port         (1 in N pkts)    (bytes)       (secs)
-----------------------------------------------------
port1.0.1            0          128             0
port1.0.2            0          128             0
port1.0.3            0          128             0
...
```

Related commands

sflow enable

show running-config sflow

show sflow

undebug sflow

Overview This command applies the functionality of the **no** variant of the debug sflow command.

69 MODBUS Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure MODBUS (Modicon Communication Bus).

MODBUS is a serial communications protocol for client-server communication between a switch (server) and a device in the network running MODBUS client software (client). You can use MODBUS to connect a computer to a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems.

The MODBUS feature allows AlliedWare Plus™ devices to be used for some SCADA processes - such as gathering sensor and alarm information and to control and monitor the state of ports and their PoE state.

The device encapsulates a request or response message in a MODBUS TCP application data unit (ADU). A client sends a message to a TCP port on the switch. The default port number is 502.

For more information, see the MODBUS Feature Overview and Configuration Guide.

Command List

- "clear scada modbus tcp server connection" on page 3313
- "clear scada modbus tcp server statistics" on page 3314
- "scada modbus tcp server access" on page 3315
- "scada modbus tcp server access permit" on page 3316
- "scada modbus tcp server connection" on page 3317
- "scada modbus tcp server port" on page 3318
- "scada modbus tcp server" on page 3319
- "show scada modbus tcp server connections" on page 3320
- "show scada modbus tcp server" on page 3322

clear scada modbus tcp server connection

Overview Use this command to forcefully disconnect a MODBUS client that is currently connected to the MODBUS TCP server.

Syntax

```
clear scada modbus tcp server connection <ip-address> <1-65535>
```

Parameter	Description
<ip-address>	The IPv4 or IPv6 address of the MODBUS TCP server.
<1-65535>	The port ID number.

Mode Privileged Exec

Example To forcefully disconnect a client from the MODBUS TCP server, use the following commands:

```
awplus# configure terminal
awplus(config)# clear scada modbus tcp server connection
198.51.100.200 33229
```

Related commands

scada modbus tcp server port

scada modbus tcp server connection

show scada modbus tcp server

scada modbus tcp server access

clear scada modbus tcp server statistics

show scada modbus tcp server connections

Command changes

Version 5.4.8-2.1: command added

Version 5.4.9-0.1: MODBUS support added for x930, x950 series

Version 5.5.0-1.1: MODBUS support added for IE510 series

clear scada modbus tcp server statistics

Overview Use this command to reset the MODBUS TCP server statistics.

Syntax

```
clear scada modbus tcp server statistics
```

Mode Privileged Exec

Example To clear the MODBUS TCP server statistics, use the following commands:

```
awplus# configure terminal
awplus(config)# clear scada modbus tcp server statistics
```

Related commands

scada modbus tcp server port

scada modbus tcp server

scada modbus tcp server connection

scada modbus tcp server access

clear scada modbus tcp server connection

show scada modbus tcp server

show scada modbus tcp server connections

Command changes

Version 5.4.8-2.1: command added

Version 5.4.9-0.1: MODBUS support added for x930, x950 series

Version 5.5.0-1.1: MODBUS support added for IE510 series

scada modbus tcp server access

Overview Use this command to configure the type of requests that are allowed to be made to the MODBUS TCP server.

Use the **no** variant of this command to revert to the default of read-only.

Syntax

```
scada modbus tcp server access {read-only|read-write}
no scada modbus tcp server access
```

Default Read-only.

Mode Global Configuration

Example To allow read and write requests to the MODBUS TCP server, use the following commands:

```
awplus# configure terminal
awplus(config)# scada modbus tcp server access read-write
```

To change from read-write access back to the default of read-only, use the following commands:

```
awplus# configure terminal
awplus(config)# no scada modbus tcp server access
```

Related commands

scada modbus tcp server port

scada modbus tcp server connection

show scada modbus tcp server

clear scada modbus tcp server connection

clear scada modbus tcp server statistics

show scada modbus tcp server connections

Command changes

Version 5.4.8-2.1: command added

Version 5.4.9-0.1: MODBUS support added for x930, x950 series

Version 5.5.0-1.1: MODBUS support added for IE510 series

scada modbus tcp server access permit

Overview Use this command to limit access to a MODBUS TCP server to specific IP addresses.

When no permitted IP addresses are configured, then any IP address can connect to the MODBUS TCP server.

When permitted IP addresses are configured, only those IP addresses will be allowed to connect to the MODBUS TCP server. All other IP addresses will be rejected.

Use the **no** variant of this command to remove an IP address from the list of permitted addresses.

Syntax

```
scada modbus tcp server access permit <ip-address>
no scada modbus tcp server access permit
```

Parameter	Description
<ip-address>	The IPv4 or IPv6 address to permit.

Default No IP addresses are configured.

Mode Global Configuration

Example To allow only 192.168.2.200 to use the MODBUS TCP server, use the following commands:

```
awplus# configure terminal
awplus(config)# scada modbus tcp server access permit
192.168.2.200
```

To remove 192.168.2.200 from the permitted MODBUS TCP server client IP addresses, use the following commands:

```
awplus# configure terminal
awplus(config)# no scada modbus tcp server access permit
192.168.2.200
```

Related commands

scada modbus tcp server port

scada modbus tcp server connection

show scada modbus tcp server

clear scada modbus tcp server connection

clear scada modbus tcp server statistics

show scada modbus tcp server connections

Command changes Version 5.4.9-0.1: command added

Version 5.5.0-1.1: MODBUS support added for IE510 series

scada modbus tcp server connection

Overview Use this command to configure the maximum number of concurrent MODBUS TCP clients allowed to be connected to the MODBUS TCP server.

Use the **no** variant of this command to revert to the default of 1.

Syntax

```
scada modbus tcp server connection <1-5>
no scada modbus tcp server connection
```

Parameter	Description
<1-5>	The maximum number of concurrent MODBUS TCP clients allowed to be connected to the MODBUS TCP server.

Default 1

Mode Global Configuration

Example To configure the maximum limit of MODBUS TCP clients to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# scada modbus tcp server connection 5
```

To reset the maximum limit of the MODBUS TCP clients back to the default of 1, use the following commands:

```
awplus# configure terminal
awplus(config)# no scada modbus tcp server connection
```

Related commands

scada modbus tcp server port

show scada modbus tcp server

scada modbus tcp server access

clear scada modbus tcp server connection

clear scada modbus tcp server statistics

show scada modbus tcp server connections

Command changes Version 5.4.8-2.1: command added

Version 5.4.9-0.1: MODBUS support added for x930, x950 series

Version 5.5.0-1.1: MODBUS support added for IE510 series

scada modbus tcp server port

Overview Use this command to set the port of the MODBUS TCP server on a device. Clients will use this port to connect to the MODBUS TCP server.

Use the **no** variant of this command to disable MODBUS TCP.

Syntax

```
scada modbus tcp server port <0-65535>
no scada modbus tcp server
```

Parameter	Description
<0-65535>	The port number of the MODBUS TCP server

Default Port 502

Mode Global Configuration

Example To configure port number 34567 as the MODBUS TCP server, use the following commands:

```
awplus# configure terminal
awplus(config)# scada modbus tcp server port 34567
```

To reset the port number of the MODBUS TCP server to the default of 502, use the following commands:

```
awplus# configure terminal
awplus(config)# no scada modbus tcp server port
```

Related commands

show scada modbus tcp server

scada modbus tcp server connection

scada modbus tcp server access

clear scada modbus tcp server connection

clear scada modbus tcp server statistics

show scada modbus tcp server connections

Command changes

Version 5.4.8-2.1: command added

Version 5.4.9-0.1: MODBUS support added for x930, x950 series

Version 5.5.0-1.1: MODBUS support added for IE510 series

scada modbus tcp server

Overview Use this command to enable MODBUS TCP server on a device.

Use the **no** variant of this command to disable MODBUS TCP.

Syntax

```
scada modbus tcp server
no scada modbus tcp server
```

Default Disabled

Mode Global Configuration

Example To enable the MODBUS TCP server, use the following commands:

```
awplus# configure terminal
awplus(config)# scada modbus tcp server
```

Related commands

scada modbus tcp server port

scada modbus tcp server connection

clear scada modbus tcp server connection

clear scada modbus tcp server statistics

show scada modbus tcp server connections

Command changes

Version 5.4.8-2.1: command added

Version 5.4.9-0.1: MODBUS support added for x930, x950 series

Version 5.5.0-1.1: MODBUS support added for IE510 series

show scada modbus tcp server connections

Overview Use this command to display the information and statistics of the currently connected clients to a MODBUS TCP server.

Syntax

```
show scada modbus tcp server connections
```

Mode User Exec and Privileged Exec

Example To display the information and statistics of the currently connected clients to a MODBUS TCP server, use the following commands:

```
awplus# configure terminal
awplus(config)# show scada modbus tcp server connections
```

Output Figure 69-1: Example output from **show scada modbus tcp server connections**

```
SCADA MODBUS Client Information

Connected client 1
  IP address      : 192.168.2.200
  Port            : 37509
  Uptime          : 22
Statistics:
  Read Requests:
    coils               :          0
    discrete inputs     :          0
    holding registers   :          2
    input registers     :          0

  Write Requests:
    single coil         :          0
    single register     :          0
    multiple coils      :          0
    multiple registers  :          0

  Other Requests        :          0

  Exceptions:
    illegal function    :          0
    illegal data address :          0
    illegal data value  :          0
    slave device failure :          0
...
```

Related commands

scada modbus tcp server port

scada modbus tcp server connection

show scada modbus tcp server

clear scada modbus tcp server connection

clear scada modbus tcp server statistics

scada modbus tcp server access

Command changes

Version 5.4.8-2.1: command added

Version 5.4.9-0.1: MODBUS support added for x930, x950 series

Version 5.5.0-1.1: MODBUS support added for IE510 series

show scada modbus tcp server

Overview Use this command to show the MODBUS TCP server information and statistics.

Syntax

```
show scada modbus tcp server
```

Mode User Exec and Privileged Exec

Example To display the MODBUS TCP server information and statistics, use the following commands:

```
awplus# configure terminal
awplus(config)# show scada modbus tcp server
```

Output Figure 69-2: Example output from **show scada modbus tcp server**

```
SCADA MODBUS Summary Information

MODBUS is enabled for this device
Write access: enabled
Master heartbeat status: Not set
Master heartbeat timeout: 0
-------------------------------------
TCP Server Characteristics:
  Port             :   502
  Max Connections :     5
Permitted IP addresses:
   192.168.2.200
   2001:db8::1
-------------------------------------
Statistics:
  Read Requests:
    coils                :          0
    discrete inputs      :          0
    holding registers    :          3
    input registers      :          0

  Write Requests:
    single coil          :          0
    single register      :          0
    multiple coils       :          0
    multiple registers   :          0

  Other Requests         :          0

  Exceptions:
    illegal function     :          0
    illegal data address :          0
    illegal data value   :          1
    slave device failure :          0
```

Related commands

scada modbus tcp server port

scada modbus tcp server connection

scada modbus tcp server access

clear scada modbus tcp server connection

clear scada modbus tcp server statistics

show scada modbus tcp server connections

Command changes

Version 5.4.8-2.1: command added

Version 5.4.9-0.1: MODBUS support added for x930, x950 series

Version 5.5.0-1.1: MODBUS support added for IE510 series