Command Reference for AlliedWare Plus™ Version 5.4.5
Acknowledgments

This product includes software developed by the University of California, Berkeley and its contributors.


All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For information about this see www.openssl.org/

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

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

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

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

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

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

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

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

Chapter 1: CLI Navigation Commands ......................................................... 82
   Introduction ........................................................................................................... 82
      configure terminal ................................................................................................. 83
      disable (Privileged Exec mode) ............................................................................. 84
      do ............................................................................................................................. 85
      enable (Privileged Exec mode) ............................................................................. 86
      end ......................................................................................................................... 88
      exit ......................................................................................................................... 89
      help ....................................................................................................................... 90
      logout ................................................................................................................... 91
      show history .......................................................................................................... 92

Chapter 2: User Access Commands ............................................................... 93
   Introduction ............................................................................................................. 93
      clear line console ................................................................................................. 94
      clear line vty ......................................................................................................... 95
      enable password .................................................................................................. 96
      enable secret ....................................................................................................... 99
      exec-timeout ....................................................................................................... 102
      flowcontrol hardware (asyn/console) ..................................................................... 104
      length (asyn) ....................................................................................................... 106
      line ....................................................................................................................... 107
      privilege level ..................................................................................................... 109
      security-password history .................................................................................. 110
      security-password forced-change ......................................................................... 111
      security-password lifetime ................................................................................... 112
      security-password minimum-categories ................................................................ 113
      security-password minimum-length ..................................................................... 114
      security-password reject-expired-pwd .................................................................. 115
      security-password warning .................................................................................. 116
      service advanced-vty ............................................................................................ 117
# File Management Commands

Chapter 3: File Management Commands .......................... 133

## Introduction ...................................................... 133

- autoboot enable ........................................ 136
- boot config-file .......................................... 137
- boot config-file backup .................................. 139
- boot system ................................................. 140
- boot system backup ....................................... 142
- cd ............................................................. 143
- copy current-software ..................................... 144
- copy debug ................................................. 145
- copy running-config ....................................... 146
- copy startup-config ....................................... 147
- copy (filename) ........................................... 148
- copy zmodem .............................................. 150
- create autoboot .......................................... 151
- delete ....................................................... 152
- delete debug .............................................. 153
- dir .......................................................... 154
- edit ......................................................... 156
- edit (filename) ........................................... 157
- erase startup-config ...................................... 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 access-list ....................... 175
- show running-config as-path access-list ............. 176
- show running-config dhcp ............................... 177
- show running-config full ................................ 178
- show running-config interface ......................... 179
- show running-config ip pim dense-mode ............. 182
- show running-config ip pim sparse-mode ............. 183
show running-config ip route ................................................. 184
show running-config ipv6 access-list .................................... 185
show running-config ipv6 mroute ......................................... 186
show running-config ipv6 prefix-list .................................... 187
show running-config ipv6 route ........................................... 188
show running-config key chain .......................................... 189
show running-config ldp .................................................. 190
show running-config power-inline ....................................... 191
show running-config prefix-list ......................................... 192
show running-config route-map .......................................... 193
show running-config router .............................................. 194
show running-config router-id ............................................ 195
show running-config security-password ............................... 196
show startup-config ...................................................... 197
show version .............................................................. 198
write file ................................................................. 200
write memory ............................................................. 201
write terminal .................................................................. 202

Chapter 4: Licensing Commands .................................................. 203
Introduction .................................................................... 203
license .......................................................................... 204
license member (deleted) .................................................... 206
show license ................................................................. 207
show license brief .......................................................... 209
show license member ....................................................... 211
show license brief member ................................................ 213

Chapter 5: System Configuration and Monitoring Commands .............. 215
Introduction .................................................................... 215
banner exec .................................................................... 216
banner login (system) ....................................................... 218
banner motd .................................................................... 220
clock set ....................................................................... 222
clock summer-time date .................................................... 223
clock summer-time recurring ............................................ 225
clock timezone .............................................................. 227
continuous-reboot-prevention ........................................... 228
default-ipv6-router-advertisement ..................................... 230
default-route .................................................................. 232
default-list ..................................................................... 234
default-ipv6-list ............................................................. 236
default-ipv6-router-advertisement ..................................... 238
ecofriendly lpi .................................................................. 231
ecofriendly led .............................................................. 233
hostname ....................................................................... 235
max-fib-routes ................................................................ 237
max-static-routes ............................................................ 238
no debug all ................................................................... 239
reboot ........................................................................... 240
reload ............................................................................ 241
show clock .................................................................... 242
show continuous-reboot-prevention ..................................... 244
show cpu ....................................................................... 245
show cpu history ............................................................. 248
show debugging ............................................................. 251
### Chapter 6: Logging Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ecofriendly</td>
<td>252</td>
</tr>
<tr>
<td>show interface memory</td>
<td>254</td>
</tr>
<tr>
<td>show memory</td>
<td>256</td>
</tr>
<tr>
<td>show memory allocations</td>
<td>258</td>
</tr>
<tr>
<td>show memory history</td>
<td>260</td>
</tr>
<tr>
<td>show memory pools</td>
<td>262</td>
</tr>
<tr>
<td>show memory shared</td>
<td>263</td>
</tr>
<tr>
<td>show process</td>
<td>264</td>
</tr>
<tr>
<td>show reboot history</td>
<td>267</td>
</tr>
<tr>
<td>show router-id</td>
<td>269</td>
</tr>
<tr>
<td>show system</td>
<td>270</td>
</tr>
<tr>
<td>show system environment</td>
<td>271</td>
</tr>
<tr>
<td>show system interrupts</td>
<td>272</td>
</tr>
<tr>
<td>show system mac</td>
<td>273</td>
</tr>
<tr>
<td>show system pci device</td>
<td>275</td>
</tr>
<tr>
<td>show system pci tree</td>
<td>276</td>
</tr>
<tr>
<td>show system pluggable</td>
<td>277</td>
</tr>
<tr>
<td>show system pluggable detail</td>
<td>280</td>
</tr>
<tr>
<td>show system pluggable diagnostics</td>
<td>285</td>
</tr>
<tr>
<td>show system serialnumber</td>
<td>288</td>
</tr>
<tr>
<td>show tech-support</td>
<td>289</td>
</tr>
<tr>
<td>speed (asyn)</td>
<td>291</td>
</tr>
<tr>
<td>system territory (deprecated)</td>
<td>293</td>
</tr>
<tr>
<td>terminal monitor</td>
<td>294</td>
</tr>
<tr>
<td>undebug all</td>
<td>295</td>
</tr>
<tr>
<td>show ecofriendly</td>
<td>252</td>
</tr>
<tr>
<td>show interface memory</td>
<td>254</td>
</tr>
<tr>
<td>show memory</td>
<td>256</td>
</tr>
<tr>
<td>show memory allocations</td>
<td>258</td>
</tr>
<tr>
<td>show memory history</td>
<td>260</td>
</tr>
<tr>
<td>show memory pools</td>
<td>262</td>
</tr>
<tr>
<td>show memory shared</td>
<td>263</td>
</tr>
<tr>
<td>show process</td>
<td>264</td>
</tr>
<tr>
<td>show reboot history</td>
<td>267</td>
</tr>
<tr>
<td>show router-id</td>
<td>269</td>
</tr>
<tr>
<td>show system</td>
<td>270</td>
</tr>
<tr>
<td>show system environment</td>
<td>271</td>
</tr>
<tr>
<td>show system interrupts</td>
<td>272</td>
</tr>
<tr>
<td>show system mac</td>
<td>273</td>
</tr>
<tr>
<td>show system pci device</td>
<td>275</td>
</tr>
<tr>
<td>show system pci tree</td>
<td>276</td>
</tr>
<tr>
<td>show system pluggable</td>
<td>277</td>
</tr>
<tr>
<td>show system pluggable detail</td>
<td>280</td>
</tr>
<tr>
<td>show system pluggable diagnostics</td>
<td>285</td>
</tr>
<tr>
<td>show system serialnumber</td>
<td>288</td>
</tr>
<tr>
<td>show tech-support</td>
<td>289</td>
</tr>
<tr>
<td>speed (asyn)</td>
<td>291</td>
</tr>
<tr>
<td>system territory (deprecated)</td>
<td>293</td>
</tr>
<tr>
<td>terminal monitor</td>
<td>294</td>
</tr>
<tr>
<td>undebug all</td>
<td>295</td>
</tr>
</tbody>
</table>
log permanent size .................................................. 338
log-rate-limit nsf .................................................... 339
show counter log .................................................... 341
show exception log ................................................... 342
show log ............................................................... 343
show log config ..................................................... 346
show log permanent ................................................ 349
show running-config log .......................................... 350

Chapter 7: Scripting Commands ........................................ 351
Introduction ......................................................... 351
activate ............................................................... 352
echo ................................................................. 353
wait ................................................................. 354

Chapter 8: Interface Commands ....................................... 355
Introduction .......................................................... 355
description (interface) ............................................ 356
interface (to configure) ........................................... 357
mtu ................................................................. 359
show interface ...................................................... 361
show interface brief ............................................... 363
show interface status ............................................. 369
shutdown ........................................................... 372

Chapter 9: Interface Testing Commands ............................ 373
Introduction .......................................................... 373
clear test interface ................................................. 374
service test .......................................................... 375
test interface ....................................................... 376

Chapter 10: Switching Commands .................................... 378
Introduction .......................................................... 378
backpressure ........................................................ 379
clear loop-protection counters .................................. 381
clear mac address-table static ................................... 382
clear mac address-table dynamic ................................ 383
clear port counter .................................................. 385
debug loopprot ..................................................... 386
debug platform packet ............................................. 387
duplex ............................................................... 389
flowcontrol (switch port) ......................................... 390
linkflap action ..................................................... 392
loop-protection ..................................................... 393
loop-protection action ............................................. 395
loop-protection action-delay-time ............................... 396
loop-protection timeout .......................................... 397
mac address-table acquire ....................................... 398
mac address-table ageing-time .................................. 399
mac address-table static ......................................... 400
mac address-table thrash-limit .................................. 401
Chapter 11: VLAN Commands ............................................. 444

Introduction ................................................................. 444
  clear vlan statistics ................................................. 445
  port-vlan-forwarding-priority .................................... 446
  private-vlan .......................................................... 449
  private-vlan association .......................................... 450
  show port-vlan-forwarding-priority ............................ 451
  show vlan ............................................................... 452
  show vlan classifier group ....................................... 453
  show vlan classifier group interface ......................... 454
  show vlan classifier interface group ......................... 455
  show vlan classifier rule ......................................... 456
  show vlan private-vlan ............................................ 457
  show vlan statistics ................................................. 458
  switchport access vlan ............................................ 459
  switchport enable vlan ............................................ 460
  switchport mode access ........................................... 461
  switchport mode private-vlan .................................... 462
  switchport mode private-vlan trunk promiscuous ............ 463
  switchport mode private-vlan trunk secondary ............... 465
  switchport mode trunk ............................................. 467

mirror interface .......................................................... 402
platform hwfilter-size ................................................. 404
platform load-balancing .............................................. 405
platform stop-unreg-mc-flooding ................................ 406
platform vlan-stacking-tpid ....................................... 408
polarity .................................................................... 409
show debugging loopprot .............................................. 410
show debugging platform packet .................................... 411
show flowcontrol interface .......................................... 412
show interface err-disabled ......................................... 413
show interface switchport ............................................ 414
show loop-protection ................................................... 415
show mac address-table .............................................. 417
show mac address-table thrash-limit ............................. 419
show mirror ............................................................... 420
show mirror interface ................................................ 421
show platform .......................................................... 422
show platform classifier statistics utilization brief ........... 423
show platform port ..................................................... 425
show port-security interface ........................................ 429
show port-security intrusion ......................................... 430
show storm-control ..................................................... 431
speed ...................................................................... 433
storm-control level .................................................... 435
switchport port-security ............................................. 436
switchport port-security aging ..................................... 437
switchport port-security maximum .................................. 438
switchport port-security violation ............................... 439
thrash-limiting .......................................................... 440
undebug loopprot ....................................................... 442
undebug platform packet .............................................. 443

AlliedWare Plus™ Operating System - Version 5.4.5-0.x
switchport private-vlan host-association ........................................ 468
switchport private-vlan mapping .................................................... 469
switchport trunk allowed vlan ....................................................... 470
switchport trunk native vlan ......................................................... 473
switchport vlan-stacking (double tagging) ...................................... 475
switchport voice dscp ................................................................. 476
switchport voice vlan ................................................................ 477
switchport voice vlan priority ......................................................... 480
vlan ...................................................................................... 481
vlan classifier activate ................................................................. 482
vlan classifier group ................................................................. 483
vlan classifier rule ipv4 ............................................................... 484
vlan classifier rule proto ............................................................ 485
vlan database .......................................................................... 488
vlan mode stack-local-vlan .......................................................... 489
vlan statistics .......................................................................... 491

Chapter 12: Spanning Tree Commands .............................................. 493
Introduction ................................................................................. 493
clear spanning-tree statistics ....................................................... 494
clear spanning-tree detected protocols (RSTP and MSTP) ............... 495
debug mstp (RSTP and STP) ......................................................... 496
instance priority (MSTP) ............................................................. 500
instance vlan (MSTP) ................................................................. 502
region (MSTP) ........................................................................ 504
revision (MSTP) .................................................................... 505
show debugging mstp ................................................................. 506
show spanning-tree .................................................................. 507
show spanning-tree brief ............................................................ 510
show spanning-tree mst .............................................................. 511
show spanning-tree mst config .................................................... 512
show spanning-tree mst detail ...................................................... 513
show spanning-tree mst detail interface ...................................... 515
show spanning-tree mst instance .................................................. 517
show spanning-tree mst instance interface .................................... 518
show spanning-tree mst interface .................................................. 519
show spanning-tree mst detail interface ........................................ 520
show spanning-tree statistics ....................................................... 522
show spanning-tree statistics instance ........................................ 524
show spanning-tree statistics instance interface ............................ 526
show spanning-tree statistics interface ........................................ 528
show spanning-tree vlan range-index .......................................... 532
spanning-tree autoedge (RSTP and MSTP) .................................... 533
spanning-tree bpdu ................................................................... 534
spanning-tree cisco-interoperability (MSTP) ................................ 536
spanning-tree edgeport (RSTP and MSTP) .................................... 537
spanning-tree enable ................................................................. 538
spanning-tree errdisable-timeout enable ....................................... 540
spanning-tree errdisable-timeout interval ..................................... 541
spanning-tree force-version ......................................................... 542
spanning-tree forward-time ......................................................... 543
spanning-tree guard root ............................................................ 544
spanning-tree hello-time ............................................................ 545
<table>
<thead>
<tr>
<th>Chapter 13:</th>
<th>Link Aggregation Commands</th>
<th>571</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>571</td>
<td></td>
</tr>
<tr>
<td>channel-group</td>
<td>572</td>
<td></td>
</tr>
<tr>
<td>clear lacp counters</td>
<td>574</td>
<td></td>
</tr>
<tr>
<td>debug lacp</td>
<td>575</td>
<td></td>
</tr>
<tr>
<td>lacp port-priority</td>
<td>576</td>
<td></td>
</tr>
<tr>
<td>lacp system-priority</td>
<td>577</td>
<td></td>
</tr>
<tr>
<td>lacp timeout</td>
<td>578</td>
<td></td>
</tr>
<tr>
<td>show debugging lacp</td>
<td>580</td>
<td></td>
</tr>
<tr>
<td>show diagnostic channel-group</td>
<td>581</td>
<td></td>
</tr>
<tr>
<td>show etherchannel</td>
<td>583</td>
<td></td>
</tr>
<tr>
<td>show etherchannel detail</td>
<td>584</td>
<td></td>
</tr>
<tr>
<td>show etherchannel summary</td>
<td>585</td>
<td></td>
</tr>
<tr>
<td>show lacp sys-id</td>
<td>586</td>
<td></td>
</tr>
<tr>
<td>show lacp-counter</td>
<td>587</td>
<td></td>
</tr>
<tr>
<td>show port etherchannel</td>
<td>588</td>
<td></td>
</tr>
<tr>
<td>show static-channel-group</td>
<td>590</td>
<td></td>
</tr>
<tr>
<td>static-channel-group</td>
<td>591</td>
<td></td>
</tr>
<tr>
<td>undebug lacp</td>
<td>593</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 14:</th>
<th>Power over Ethernet Commands</th>
<th>594</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>594</td>
<td></td>
</tr>
<tr>
<td>clear power-inline counters interface</td>
<td>595</td>
<td></td>
</tr>
<tr>
<td>debug power-inline</td>
<td>596</td>
<td></td>
</tr>
<tr>
<td>power-inline allow-legacy</td>
<td>598</td>
<td></td>
</tr>
<tr>
<td>power-inline description</td>
<td>599</td>
<td></td>
</tr>
<tr>
<td>power-inline enable</td>
<td>600</td>
<td></td>
</tr>
<tr>
<td>power-inline max</td>
<td>601</td>
<td></td>
</tr>
<tr>
<td>power-inline priority</td>
<td>603</td>
<td></td>
</tr>
<tr>
<td>power-inline usage-threshold</td>
<td>605</td>
<td></td>
</tr>
<tr>
<td>service power-inline</td>
<td>606</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 16: IP Addressing and Protocol Commands ........................................... 633

Introduction ........................................................................................................... 633
arp-aging-timeout .................................................................................................... 634
arp-mac-disparity .................................................................................................... 635
arp (IP address MAC) .............................................................................................. 636
arp log ...................................................................................................................... 637
arp opportunistic-nd ............................................................................................... 640
clear arp-cache ......................................................................................................... 641
clear ip dns forwarding cache ................................................................................ 642
dbg ip dns forwarding ............................................................................................... 643
dbg ip packet interface ............................................................................................. 644
ip address ................................................................................................................ 646
ip directed-broadcast ............................................................................................... 648
ip dns forwarding .................................................................................................... 650
ip dns forwarding cache .......................................................................................... 651
ip dns forwarding dead-time ................................................................................... 652
ip dns forwarding retry ......................................................................................... 653
ip dns forwarding source-interface ....................................................................... 654
ip dns forwarding timeout ...................................................................................... 655
ip domain-list ......................................................................................................... 656
ip domain-lookup .................................................................................................... 657
ip domain-name ....................................................................................................... 658
ip forward-protocol udp .......................................................................................... 659
ip gratuitous-arp-link .............................................................................................. 660
ip helper-address .................................................................................................... 661
ip local-proxy-arp .................................................................................................... 663
ip name-server ........................................................................................................ 665
ip proxy-arp ............................................................................................................. 666
ip redirects ............................................................................................................. 668
optimistic-nd ........................................................................................................... 669
ping ......................................................................................................................... 670

Chapter 15: GVRP Commands ............................................................................... 618

Introduction .............................................................................................................. 618
clear gvrp statistics ................................................................................................. 619
debug gvrp ................................................................................................................ 620
gvrp (interface) ....................................................................................................... 622
gvrp dynamic-vlan-creation ................................................................................. 623
gvrp enable (global) ............................................................................................... 624
gvrp registration ...................................................................................................... 625
gvrp timer ................................................................................................................ 626
show debugging gvrp .............................................................................................. 628
show gvrp configuration ......................................................................................... 629
show gvrp machine ................................................................................................. 630
show gvrp statistics ............................................................................................... 631
show gvrp timer ....................................................................................................... 632
### Chapter 17: IPv6 Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show debug ipv6 neighbors</td>
<td>697</td>
</tr>
<tr>
<td>clear ipv6 neighbors</td>
<td>697</td>
</tr>
<tr>
<td>ipv6 address</td>
<td>698</td>
</tr>
<tr>
<td>ipv6 address autoconfig</td>
<td>700</td>
</tr>
<tr>
<td>ipv6 enable</td>
<td>702</td>
</tr>
<tr>
<td>ipv6 forwarding</td>
<td>704</td>
</tr>
<tr>
<td>ipv6 nd managed-config-flag</td>
<td>705</td>
</tr>
<tr>
<td>ipv6 nd minimum-ra-interval</td>
<td>706</td>
</tr>
<tr>
<td>ipv6 nd other-config-flag</td>
<td>707</td>
</tr>
<tr>
<td>ipv6 nd prefix</td>
<td>708</td>
</tr>
<tr>
<td>ipv6 nd ra-interval</td>
<td>710</td>
</tr>
<tr>
<td>ipv6 nd ra-lifetime</td>
<td>711</td>
</tr>
<tr>
<td>ipv6 nd raguard</td>
<td>712</td>
</tr>
<tr>
<td>ipv6 nd reachable-time</td>
<td>714</td>
</tr>
<tr>
<td>ipv6 nd retransmission-time</td>
<td>715</td>
</tr>
<tr>
<td>ipv6 nd suppress-ra</td>
<td>716</td>
</tr>
<tr>
<td>ipv6 neighbor</td>
<td>717</td>
</tr>
<tr>
<td>ipv6 opportunistic-nd</td>
<td>718</td>
</tr>
<tr>
<td>ipv6 route</td>
<td>719</td>
</tr>
<tr>
<td>ping ipv6</td>
<td>720</td>
</tr>
<tr>
<td>show ipv6 forwarding</td>
<td>721</td>
</tr>
<tr>
<td>show ipv6 interface brief</td>
<td>722</td>
</tr>
<tr>
<td>show ipv6 neighbors</td>
<td>723</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>724</td>
</tr>
<tr>
<td>show ipv6 route summary</td>
<td>726</td>
</tr>
<tr>
<td>traceroute ipv6</td>
<td>727</td>
</tr>
</tbody>
</table>

### Chapter 18: Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show arp</td>
<td>671</td>
</tr>
<tr>
<td>show debugging ipv6 forwarding</td>
<td>673</td>
</tr>
<tr>
<td>show debugging ip packet</td>
<td>674</td>
</tr>
<tr>
<td>show hosts</td>
<td>676</td>
</tr>
<tr>
<td>show ip forwarding</td>
<td>677</td>
</tr>
<tr>
<td>show ip forwarding cache</td>
<td>678</td>
</tr>
<tr>
<td>show ip forwarding server</td>
<td>679</td>
</tr>
<tr>
<td>show ip domain-list</td>
<td>680</td>
</tr>
<tr>
<td>show ip domain-name</td>
<td>681</td>
</tr>
<tr>
<td>show ip interface</td>
<td>682</td>
</tr>
<tr>
<td>show ip name-server</td>
<td>683</td>
</tr>
<tr>
<td>show ip sockets</td>
<td>684</td>
</tr>
<tr>
<td>show ip traffic</td>
<td>687</td>
</tr>
<tr>
<td>tcpdump</td>
<td>693</td>
</tr>
<tr>
<td>traceroute</td>
<td>694</td>
</tr>
<tr>
<td>und debug ip packet interface</td>
<td>695</td>
</tr>
</tbody>
</table>

### Chapter 18: Routing Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip traffic</td>
<td>687</td>
</tr>
<tr>
<td>show ip sockets</td>
<td>684</td>
</tr>
<tr>
<td>show ip name-server</td>
<td>683</td>
</tr>
<tr>
<td>show ip domain-name</td>
<td>681</td>
</tr>
<tr>
<td>show ip interface</td>
<td>682</td>
</tr>
<tr>
<td>show ip name-server</td>
<td>683</td>
</tr>
<tr>
<td>show ip sockets</td>
<td>684</td>
</tr>
<tr>
<td>show ip traffic</td>
<td>687</td>
</tr>
<tr>
<td>tcpdump</td>
<td>693</td>
</tr>
<tr>
<td>traceroute</td>
<td>694</td>
</tr>
<tr>
<td>und debug ip packet interface</td>
<td>695</td>
</tr>
</tbody>
</table>
Chapter 20: RIPng for IPv6 Commands ........................................... 791

Introduction ................................................................. 791
aggregate-address (IPv6 RIPng) ......................................... 792
clear ipv6 rip route ...................................................... 793
debug ipv6 rip ............................................................ 794
default-information originate (IPv6 RIPng) ......................... 795
default-metric (IPv6 RIPng) ............................................. 796

Chapter 19: RIP Commands .................................................. 738

Introduction ..................................................................... 738
accept-lifetime .................................................................. 739
alliedware-behavior ......................................................... 741
cisco-metric-behavior (RIP) .............................................. 743
clear ip rip route ............................................................ 744
debug rip ........................................................................ 745
default-information originate (RIP) ................................. 746
default-metric (RIP) ......................................................... 747
distance (RIP) ................................................................. 748
distribute-list (RIP) ......................................................... 749
fullupdate (RIP) .............................................................. 750
ip rip authentication key-chain .......................................... 751
ip rip authentication mode ................................................ 753
ip rip authentication string ................................................ 756
ip rip receive-packet ....................................................... 758
ip rip receive version ...................................................... 759
ip rip send-packet ........................................................... 760
ip rip send version .......................................................... 761
ip rip send version 1-compatible ....................................... 763
ip rip split-horizon .......................................................... 765
key .............................................................................. 766
key chain ....................................................................... 767
key-string ..................................................................... 768
maximum-prefix ............................................................. 769
neighbor (RIP) ................................................................. 770
network (RIP) ................................................................ 771
offset-list (RIP) ............................................................... 772
passive-interface (RIP) ...................................................... 773
recv-buffer-size (RIP) ....................................................... 774
redistribute (RIP) ............................................................ 775
restart rip graceful .......................................................... 776
rip restart grace-period .................................................... 777
route (RIP) ..................................................................... 778
router rip ....................................................................... 779
send-lifetime ................................................................... 780
show debugging rip .......................................................... 782
show ip protocols rip ....................................................... 783
show ip rip ..................................................................... 784
show ip rip database ........................................................ 785
show ip rip interface ........................................................ 786
timers (RIP) ................................................................... 787
undebug rip ..................................................................... 789
version ......................................................................... 790
Chapter 21: OSPF Commands

Introduction ......................................................... 816
area default-cost .................................................. 817
area authentication ............................................... 818
area filter-list ...................................................... 819
area nssa ........................................................... 820
area range .......................................................... 822
area stub ............................................................ 824
area virtual-link .................................................. 825
auto-cost reference bandwidth ................................. 828
bandwidth .......................................................... 830
capability opaque .................................................. 831
capability restart .................................................. 832
clear ip ospf process .............................................. 833
compatible rfc1583 ............................................... 834
debug ospf events ................................................ 835
debug ospf ifsm .................................................... 836
debug ospf lsa ...................................................... 837
debug ospf nfsm ................................................... 838
debug ospf nsm ..................................................... 839
debug ospf packet ................................................ 840
debug ospf route ................................................... 841
default-information originate (OSPF) ......................... 842
default-metric (OSPF) ............................................ 843
distance (OSPF) ................................................... 844
distribute-list (OSPF) ............................................ 846
enable db-summary-opt ........................................ 848
host area .......................................................... 849
ip ospf authentication ............................................ 850
ip ospf authentication-key ..................................... 851
ip ospf cost ......................................................... 852
ip ospf database-filter ........................................... 853
ip ospf dead-interval ............................................. 854
ip ospf disable all ............................................... 855
Chapter 22: OSPFv3 for IPv6 Commands ........................................... 920
Chapter 26: MLD and MLD Snooping Commands

MLD and MLD Snooping Commands

Introduction

clear ipv6 mld

clear ipv6 mld group

clear ipv6 mld interface

debug mld

ipv6 mld

ipv6 mld access-group

ipv6 mld immediate-leave

ipv6 mld last-member-query-count

ipv6 mld last-member-query-interval

ipv6 mld limit

ipv6 mld mroute-proxy

ipv6 mld proxy-service

ipv6 mld querier-timeout

ipv6 mld query-holdtime

ipv6 mld query-interval

ipv6 mld query-max-response-time

ipv6 mld ra-option (Router Alert)

ipv6 mld robustness-variable

ipv6 mld snooping

ipv6 mld snooping fast-leave

ipv6 mld snooping mrouter

ipv6 mld snooping querier

ipv6 mld snooping report-suppression

ipv6 mld snooping routermode

ipv6 mld snooping tcn query-solicit

ipv6 mld source-address-check

ipv6 mld ssm

ipv6 mld ssm-map enable

ipv6 mld ssm-map static

ipv6 mld static-group

ipv6 mld startup-query-count

ipv6 mld startup-query-interval

ipv6 mld version

show debugging igmp

show ip igmp groups

show ip igmp interface

show ip igmp proxy

show ip igmp snooping mrouter

show ip igmp snooping routermode

show ip igmp snooping statistics

undebug igmp

show ip igmp snooping tcn query-solicit

show ip igmp snooping routermode

show ip igmp snooping quota

show ip igmp snooping limit
# Chapter 27: PIM-SM Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip pim ssm</td>
<td>1189</td>
</tr>
<tr>
<td>ip pim spt-threshold group-list</td>
<td>1188</td>
</tr>
<tr>
<td>ip pim spt-threshold</td>
<td>1187</td>
</tr>
<tr>
<td>ip pim sparse-mode</td>
<td>1186</td>
</tr>
<tr>
<td>ip pim accept-register list</td>
<td>1162</td>
</tr>
<tr>
<td>ip pim register-suppression</td>
<td>1180</td>
</tr>
<tr>
<td>ip pim register-source</td>
<td>1179</td>
</tr>
<tr>
<td>ip pim register-rp-reachability</td>
<td>1178</td>
</tr>
<tr>
<td>ip pim register-rate-limit</td>
<td>1177</td>
</tr>
<tr>
<td>ip pim neighbor-filter (PIM-SM)</td>
<td>1176</td>
</tr>
<tr>
<td>ip pim ignore-rp-set-priority</td>
<td>1174</td>
</tr>
<tr>
<td>ip pim jp-timer</td>
<td>1175</td>
</tr>
<tr>
<td>ip pim hello-interval (PIM-SM)</td>
<td>1172</td>
</tr>
<tr>
<td>ip pim hello-_holdtime (PIM-SM)</td>
<td>1171</td>
</tr>
<tr>
<td>ip pim static-group</td>
<td>1148</td>
</tr>
<tr>
<td>ip pim rp-candidate</td>
<td>1183</td>
</tr>
<tr>
<td>ip pim rp-address</td>
<td>1181</td>
</tr>
<tr>
<td>ip pim rp-candidate</td>
<td>1183</td>
</tr>
<tr>
<td>ip pim rp-register-kat</td>
<td>1184</td>
</tr>
<tr>
<td>ip pim sparse-mode</td>
<td>1185</td>
</tr>
<tr>
<td>ip pim passive</td>
<td>1186</td>
</tr>
<tr>
<td>ip mld version</td>
<td>1150</td>
</tr>
<tr>
<td>clear ip mroute pim sparse-mode</td>
<td>1158</td>
</tr>
<tr>
<td>debug pim sparse-mode timer</td>
<td>1160</td>
</tr>
<tr>
<td>ip pim dr-priority</td>
<td>1159</td>
</tr>
<tr>
<td>ip pim exclude-genid</td>
<td>1169</td>
</tr>
<tr>
<td>ipv6 mld last-member-query-interval</td>
<td>1133</td>
</tr>
<tr>
<td>ipv6 mld limit</td>
<td>1134</td>
</tr>
<tr>
<td>ipv6 mld querier-timeout</td>
<td>1136</td>
</tr>
<tr>
<td>ipv6 mld query-interval</td>
<td>1137</td>
</tr>
<tr>
<td>ipv6 mld query-max-response-time</td>
<td>1138</td>
</tr>
<tr>
<td>ipv6 mld robustness-variable</td>
<td>1139</td>
</tr>
<tr>
<td>ipv6 mld snooping</td>
<td>1140</td>
</tr>
<tr>
<td>ipv6 mld snooping fast-leave</td>
<td>1142</td>
</tr>
<tr>
<td>ipv6 mld snooping mrouter</td>
<td>1143</td>
</tr>
<tr>
<td>ipv6 mld snooping querier</td>
<td>1145</td>
</tr>
<tr>
<td>ipv6 mld snooping report-suppression</td>
<td>1146</td>
</tr>
<tr>
<td>ipv6 mld static-group</td>
<td>1148</td>
</tr>
<tr>
<td>show debugging mld</td>
<td>1151</td>
</tr>
<tr>
<td>show ipv6 mld groups</td>
<td>1152</td>
</tr>
<tr>
<td>show ipv6 mld interface</td>
<td>1153</td>
</tr>
<tr>
<td>show ipv6 mld snooping mrouter</td>
<td>1154</td>
</tr>
<tr>
<td>show ipv6 mld snooping statistics</td>
<td>1155</td>
</tr>
<tr>
<td>show ipv6 mld snooping mrouter</td>
<td>1154</td>
</tr>
<tr>
<td>show ipv6 mld interface</td>
<td>1153</td>
</tr>
<tr>
<td>show ipv6 mld groups</td>
<td>1152</td>
</tr>
<tr>
<td>show debugging mld</td>
<td>1151</td>
</tr>
<tr>
<td>show ipv6 mld snooping statistics</td>
<td>1155</td>
</tr>
<tr>
<td>show ipv6 mld snooping mrouter</td>
<td>1154</td>
</tr>
<tr>
<td>show ipv6 mld interface</td>
<td>1153</td>
</tr>
<tr>
<td>show ipv6 mld groups</td>
<td>1152</td>
</tr>
<tr>
<td>show debugging mld</td>
<td>1151</td>
</tr>
<tr>
<td>ipv6 mld last-member-query-interval</td>
<td>1133</td>
</tr>
<tr>
<td>ipv6 mld limit</td>
<td>1134</td>
</tr>
<tr>
<td>ipv6 mld querier-timeout</td>
<td>1136</td>
</tr>
<tr>
<td>ipv6 mld query-interval</td>
<td>1137</td>
</tr>
<tr>
<td>ipv6 mld query-max-response-time</td>
<td>1138</td>
</tr>
<tr>
<td>ipv6 mld robustness-variable</td>
<td>1139</td>
</tr>
<tr>
<td>ipv6 mld snooping</td>
<td>1140</td>
</tr>
<tr>
<td>ipv6 mld snooping fast-leave</td>
<td>1142</td>
</tr>
<tr>
<td>ipv6 mld snooping mrouter</td>
<td>1143</td>
</tr>
<tr>
<td>ipv6 mld snooping querier</td>
<td>1145</td>
</tr>
<tr>
<td>ipv6 mld snooping report-suppression</td>
<td>1146</td>
</tr>
<tr>
<td>ipv6 mld static-group</td>
<td>1148</td>
</tr>
<tr>
<td>ipv6 mld version</td>
<td>1150</td>
</tr>
<tr>
<td>show debugging mld</td>
<td>1151</td>
</tr>
<tr>
<td>show ipv6 mld groups</td>
<td>1152</td>
</tr>
<tr>
<td>show ipv6 mld interface</td>
<td>1153</td>
</tr>
<tr>
<td>show ipv6 mld snooping mrouter</td>
<td>1154</td>
</tr>
<tr>
<td>show ipv6 mld snooping statistics</td>
<td>1155</td>
</tr>
</tbody>
</table>

---

**C613-50058-01 REV A**

Command Reference for x510 Series Switches

AlliedWare Plus™ Operating System - Version 5.4.5-0.x
### Chapter 28: PIM-SMv6 Commands

<table>
<thead>
<tr>
<th>Command Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip pim sparse-mode bsr-router</td>
<td>1191</td>
</tr>
<tr>
<td>show ip pim sparse-mode interface</td>
<td>1192</td>
</tr>
<tr>
<td>show ip pim sparse-mode interface detail</td>
<td>1194</td>
</tr>
<tr>
<td>show ip pim sparse-mode local-members</td>
<td>1195</td>
</tr>
<tr>
<td>show ip pim sparse-mode mroutemap</td>
<td>1197</td>
</tr>
<tr>
<td>show ip pim sparse-mode mroutemap detail</td>
<td>1199</td>
</tr>
<tr>
<td>show ip pim sparse-mode neighbor</td>
<td>1201</td>
</tr>
<tr>
<td>show ip pim sparse-mode next-hop</td>
<td>1202</td>
</tr>
<tr>
<td>show ip pim sparse-mode rp-hash</td>
<td>1203</td>
</tr>
<tr>
<td>show ip pim sparse-mode rp mapping</td>
<td>1204</td>
</tr>
<tr>
<td>undebug all pim sparse-mode</td>
<td>1205</td>
</tr>
</tbody>
</table>

Introduction | 1206
---|---
clear ipv6 mroute pim | 1207
clear ipv6 mroute pim sparse-mode | 1208
clear ipv6 pim sparse-mode bsr rp-set | 1209
debug ipv6 pim sparse-mode | 1210
debug ipv6 pim sparse-mode packet | 1212
debug ipv6 pim sparse-mode timer | 1213
ipv6 pim accept-register | 1215
ipv6 pim anycast-rp | 1216
ipv6 pim bsr-border | 1217
ipv6 pim bsr-candidate | 1218
ipv6 pim cisco-register-checksum | 1219
ipv6 pim cisco-register-checksum group-list | 1220
ipv6 pim crp-cisco-prefix | 1221
ipv6 pim dr-priority | 1222
ipv6 pim exclude-genid | 1223
ipv6 pim ext-srcs-directly-connected | 1224
ipv6 pim hello-holdtime | 1225
ipv6 pim hello-interval | 1226
ipv6 pim ignore-rp-set-priority | 1227
ipv6 pim jp-timer | 1228
ipv6 pim neighbor-filter | 1229
ipv6 pim register-rate-limit | 1230
ipv6 pim register-rp-reachability | 1231
ipv6 pim register-source | 1232
ipv6 pim register-suppression | 1233
ipv6 pim rp-address | 1234
ipv6 pim rp-candidate | 1236
ipv6 pim rp embedded | 1238
ipv6 pim rp-register-kat | 1239
ipv6 pim sparse-mode | 1240
ipv6 pim sparse-mode passive | 1241
ipv6 pim spt-threshold | 1242
ipv6 pim spt-threshold group-list | 1243
ipv6 pim ssm | 1244
ipv6 pim unicast-bsm | 1245
show debugging ipv6 pim sparse-mode | 1246
show ipv6 pim sparse-mode bsr-router | 1247
show ipv6 pim sparse-mode interface | 1248
show ipv6 pim sparse-mode interface detail | 1250
show ipv6 pim sparse-mode local-members .......................... 1251
show ipv6 pim sparse-mode mroute ................................. 1253
show ipv6 pim sparse-mode mroute detail ....................... 1255
show ipv6 pim sparse-mode neighbor ............................ 1257
show ipv6 pim sparse-mode nexthop ............................... 1258
show ipv6 pim sparse-mode rp-hash .............................. 1259
show ipv6 pim sparse-mode rp mapping ........................... 1260
show ipv6 pim sparse-mode rp nexthop ......................... 1261
undebug all ipv6 pim sparse-mode ................................ 1263
undebug ipv6 pim sparse-mode .................................... 1264

Chapter 29: PIM-DM Commands ...................................... 1266

Introduction .......................................................... 1266
debug pim dense-mode all ........................................... 1267
debug pim dense-mode context ..................................... 1268
debug pim dense-mode decode ..................................... 1269
debug pim dense-mode encode ..................................... 1270
debug pim dense-mode fsm ......................................... 1271
debug pim dense-mode mrt .......................................... 1272
debug pim dense-mode nexthop ................................... 1273
debug pim dense-mode nsm ........................................ 1274
debug pim dense-mode vif .......................................... 1275
ip pim dense-mode .................................................. 1276
ip pim dense-mode passive ....................................... 1277
ip pim ext-srscs-directly-connected (PIM-DM) ............... 1278
ip pim hello-holdtime (PIM-DM) ................................. 1279
ip pim hello-interval (PIM-DM) ................................ 1280
ip pim max-graft-retries ......................................... 1281
ip pim neighbor-filter (PIM-DM) ................................ 1283
ip pim propagation-delay ........................................ 1284
ip pim state-refresh origination-interval ..................... 1285
show debugging pim dense-mode ................................. 1286
show ip pim dense-mode interface ............................ 1287
show ip pim dense-mode interface detail .................. 1289
show ip pim dense-mode mroute ................................ 1290
show ip pim dense-mode neighbor ................................ 1291
show ip pim dense-mode neighbor detail .................... 1292
show ip pim dense-mode nexthop ................................ 1293
undebug all pim dense-mode .................................... 1294

Chapter 30: IPv4 Hardware Access Control List (ACL) Commands .............. 1295

Introduction .......................................................... 1295
access-group .......................................................... 1297
access-list (hardware IP numbered) ................................ 1299
access-list (hardware MAC numbered) .......................... 1309
access-list hardware (named) ..................................... 1312
(access-list hardware ICMP filter) .............................. 1314
(access-list hardware IP protocol filter) ................. 1317
(access-list hardware MAC filter) .............................. 1323
(access-list hardware TCP UDP filter) ..................... 1326
commit (IPv4) ......................................................... 1329
show access-list (IPv4 Hardware ACLs) ....................... 1330
show interface access-group ........................................ 1332

Chapter 31: IPv4 Software Access Control List (ACL) Commands ............... 1333

Introduction ....................................................... 1333
access-list extended (named) .................................... 1335
access-list (extended numbered) .................................. 1343
(access-list extended ICMP filter) .............................. 1345
(access-list extended IP filter) ................................. 1347
(access-list extended IP protocol filter) ....................... 1350
(access-list extended TCP UDP filter) ......................... 1355
access-list standard (named) .................................... 1358
access-list (standard numbered) ............................... 1360
(access-list standard named filter) .......................... 1362
(access-list standard standard numbered filter) ............ 1364
clear ip prefix-list ................................................ 1366
dos ...................................................................... 1367
ip prefix-list ......................................................... 1370
maximum-access-list ............................................... 1372
show access-list (IPv4 Software ACLs) ....................... 1373
show dos interface .................................................. 1375
show ip access-list .................................................. 1378
show ip prefix-list ................................................... 1379

Chapter 32: IPv6 Hardware Access Control List (ACL) Commands .................. 1380

Introduction ....................................................... 1380
commit (IPv6) ......................................................... 1382
ipv6 access-list (named) ......................................... 1383
(ipv6 access-list named ICMP filter) ......................... 1385
(ipv6 access-list named protocol filter) ....................... 1388
(ipv6 access-list named TCP UDP filter) ..................... 1393
ipv6 traffic-filter ................................................... 1397
show ipv6 access-list (IPv6 Hardware ACLs) ............... 1399

Chapter 33: IPv6 Software Access Control List (ACL) Commands .................... 1401

Introduction ....................................................... 1401
ipv6 access-list extended (named) ............................ 1403
ipv6 access-list extended proto ............................... 1407
(ipv6 access-list extended IP protocol filter) ............... 1410
(ipv6 access-list extended TCP UDP filter) ................. 1413
ipv6 access-list standard (named) ............................ 1415
(ipv6 access-list standard filter) .............................. 1417
ipv6 prefix-list ..................................................... 1419
show ipv6 access-list (IPv6 Software ACLs) ............... 1421
show ipv6 prefix-list .............................................. 1422

Chapter 34: QoS Commands ............................................. 1423

Introduction ....................................................... 1423
class ................................................................. 1424
class-map ........................................................... 1425
clear mls qos interface policer-counters ..................... 1426
default-action ...................................................... 1427
description (QoS policy-map) ................................... 1428
Chapter 35: 802.1X Commands

egress-rate-limit .............................................. 1429
match access-group ........................................... 1430
match cos ......................................................... 1432
match dscp ......................................................... 1433
match eth-format protocol ................................. 1434
match inner-cos ............................................... 1437
match inner-vlan .............................................. 1438
match ip-precedence .......................................... 1439
match mac-type ................................................ 1440
match tcp-flags ............................................... 1441
match vlan ....................................................... 1442
mls qos cos ...................................................... 1443
mls qos enable .................................................. 1444
mls qos map cos-queue to ............................... 1445
mls qos map premark-dscp to ......................... 1446
no police .......................................................... 1448
police single-rate action ................................. 1449
police twin-rate action .................................. 1451
policy-map ....................................................... 1453
priority-queue ................................................ 1454
remark-map ....................................................... 1455
remark new-cos ............................................... 1457
service-policy input ........................................ 1459
set ip next-hop (PBR) ...................................... 1460
show class-map ............................................... 1461
show mls qos .................................................... 1462
show mls qos interface .................................. 1463
show mls qos interface policer-counters ........ 1466
show mls qos interface queue-counters .......... 1468
show mls qos interface storm-status ............ 1469
show mls qos maps cos-queue .............. 1470
show mls qos maps premark-dscp ............. 1471
show policy-map .............................................. 1472
storm-action ..................................................... 1473
storm-downtime ............................................... 1474
storm-protection ............................................. 1475
storm-rate ....................................................... 1476
storm-window .................................................. 1477
trust dscp ......................................................... 1478
wrr-queue disable queues ............................... 1479
wrr-queue egress-rate-limit queues .......... 1480
wrr-queue weight queues ............................... 1481

Chapter 35: 802.1X Commands ............................... 1482

Introduction ......................................................... 1482
debug dot1x ....................................................... 1483
dot1x control-direction .................................. 1484
dot1x eap ........................................................ 1485
dot1x eapol-version ........................................... 1486
dot1x initialize interface ............................. 1487
dot1x initialize supplicant ............................ 1488
dot1x keytransmit .............................................. 1489
dot1x max-auth-fail ........................................... 1490
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x max-reauth-req</td>
<td>1492</td>
</tr>
<tr>
<td>dot1x port-control</td>
<td>1493</td>
</tr>
<tr>
<td>dot1x timeout tx-period</td>
<td>1495</td>
</tr>
<tr>
<td>show debugging dot1x</td>
<td>1496</td>
</tr>
<tr>
<td>show dot1x</td>
<td>1497</td>
</tr>
<tr>
<td>show dot1x diagnostics</td>
<td>1500</td>
</tr>
<tr>
<td>show dot1x interface</td>
<td>1502</td>
</tr>
<tr>
<td>show dot1x sessionstatistics</td>
<td>1507</td>
</tr>
<tr>
<td>show dot1x statistics interface</td>
<td>1508</td>
</tr>
<tr>
<td>show dot1x supplicant</td>
<td>1509</td>
</tr>
<tr>
<td>show dot1x supplicant interface</td>
<td>1512</td>
</tr>
<tr>
<td>undebug dot1x</td>
<td>1515</td>
</tr>
</tbody>
</table>

**Chapter 36: Authentication Commands**

**Introduction**

auth auth-fail vlan                        1516
auth critical                              1517
auth dynamic-vlan-creation                 1519
auth guest-vlan                            1520
auth host-mode                             1523
auth log                                   1525
auth max-suppliant                         1527
auth reauthentication                      1529
auth roaming disconnected                   1530
auth roaming enable                         1531
auth supplicant-mac                        1533
auth timeout connect-timeout               1535
auth timeout quiet-period                  1537
auth timeout reauth-period                 1538
auth timeout server-timeout                1539
auth timeout supp-timeout                  1540
auth two-step enable                       1541
auth-mac enable                            1542
auth-mac method                            1545
auth-mac password                          1547
auth-mac reauth-relearning                 1548
auth-web enable                            1550
auth-web forward                           1551
auth-web forward                           1552
auth-web max-auth-fail                     1554
auth-web method                            1555
auth-web-server blocking-mode              1556
auth-web-server dhcp ipaddress             1557
auth-web-server dhcp lease                 1558
auth-web-server dhcp-wpad-option           1559
auth-web-server gateway (deleted)          1560
auth-web-server host-name                  1561
auth-web-server http-redirect (deleted)    1562
auth-web-server intercept-port             1563
auth-web-server ipaddress                  1564
auth-web-server login-url                  1565
auth-web-server mode (deleted)             1566
auth-web-server page logo                  1567
auth-web-server page sub-title             1568
Chapter 40: TACACS+ Commands ................................................. 1711
  Introduction ............................................................... 1711
  show tacacs+ .............................................................. 1712
  tacacs-server host ...................................................... 1713
  tacacs-server key ....................................................... 1715
  tacacs-server timeout .................................................. 1716

Chapter 41: Secure Shell (SSH) Commands .............................. 1717
  Introduction ............................................................... 1717
  banner login (SSH) ...................................................... 1718
  clear ssh ................................................................. 1719
  crypto key destroy hostkey ........................................... 1720
  crypto key destroy userkey ........................................... 1721
  crypto key generate hostkey ......................................... 1722
  crypto key generate userkey ......................................... 1723
  crypto key pubkey-chain knownhosts ............................... 1724
  crypto key pubkey-chain userkey ................................... 1726
  debug ssh client ....................................................... 1728
  debug ssh server ..................................................... 1729
  service ssh ............................................................. 1730
  show banner login ..................................................... 1732
  show crypto key hostkey .............................................. 1733
  show crypto key pubkey-chain knownhosts ......................... 1734
  show crypto key pubkey-chain userkey ............................ 1735
  show crypto key userkey ............................................. 1736
  show running-config ssh .............................................. 1737
  show ssh ............................................................... 1739
  show ssh client ....................................................... 1741
  show ssh server ....................................................... 1742
  show ssh server allow-users ........................................ 1744
  show ssh server deny-users ......................................... 1745
  ssh ................................................................. 1746
  ssh client ........................................................... 1748
  ssh server ........................................................... 1750
  ssh server allow-users .............................................. 1752
  ssh server authentication .......................................... 1754
  ssh server deny-users ............................................... 1756
  ssh server resolve-host ............................................. 1758
  ssh server scp ......................................................... 1759
  ssh server sftp ....................................................... 1760
  undebug ssh client ................................................... 1761
  undebug ssh server .................................................. 1762

show crypto pki certificates local-radius-all-users .................. 1697
show crypto pki certificates user ..................................... 1699
show crypto pki trustpoints ........................................... 1701
show radius local-server group ........................................ 1702
show radius local-server nas .......................................... 1703
show radius local-server statistics ................................... 1704
show radius local-server user .......................................... 1706
user (RADIUS server) .................................................... 1708
vlan (RADIUS server) .................................................... 1710
Chapter 42: DHCP Snooping Commands  ........................................ 1763
  Introduction ................................................................. 1763
  arp security ................................................................. 1764
  arp security violation .................................................... 1765
  clear arp security statistics ............................................ 1767
  clear ip dhcp snooping binding ......................................... 1768
  clear ip dhcp snooping statistics ....................................... 1769
  debug arp security ........................................................ 1770
  debug ip dhcp snooping ................................................... 1771
  ip dhcp snooping ........................................................... 1772
  ip dhcp snooping agent-option ........................................... 1773
  ip dhcp snooping agent-option allow-untrusted ..................... 1774
  ip dhcp snooping agent-option circuit-id vlantriplet ............... 1775
  ip dhcp snooping agent-option remote-id ............................ 1776
  ip dhcp snooping binding ............................................... 1777
  ip dhcp snooping database ............................................... 1778
  ip dhcp snooping delete-by-client ...................................... 1779
  ip dhcp snooping delete-by-linkdown .................................. 1780
  ip dhcp snooping max-bindings ......................................... 1781
  ip dhcp snooping subscriber-id ........................................ 1782
  ip dhcp snooping trust .................................................... 1783
  ip dhcp snooping verify mac-address ................................... 1784
  ip dhcp snooping violation ............................................... 1785
  ip source binding ........................................................ 1786
  service dhcp-snooping .................................................... 1788
  show arp security .......................................................... 1790
  show arp security interface ............................................ 1791
  show arp security statistics ............................................ 1793
  show debugging arp security ............................................ 1795
  show debugging ip dhcp snooping ....................................... 1796
  show ip dhcp snooping .................................................... 1797
  show ip dhcp snooping acl ................................................. 1798
  show ip dhcp snooping agent-option ................................... 1801
  show ip dhcp snooping binding .......................................... 1804
  show ip dhcp snooping interface ....................................... 1806
  show ip dhcp snooping statistics ...................................... 1808
  show ip source binding ................................................... 1811

Chapter 43: VRRP Commands ................................................. 1812
  Introduction ............................................................... 1812
  advertisement-interval .................................................. 1813
  circuit-failover ............................................................ 1815
  debug vrrp ................................................................. 1817
  debug vrrp events .......................................................... 1818
  debug vrrp packet ......................................................... 1819
  disable (VRRP) ............................................................... 1820
  enable (VRRP) ............................................................... 1821
  preempt-mode ............................................................... 1822
  priority ...................................................................... 1824
  router vrrp (interface) ................................................... 1826
  router ipv6 vrrp (interface) ............................................. 1827
  show debugging vrrp ........................................................ 1828
<table>
<thead>
<tr>
<th>Chapter 44:</th>
<th>EPSR Commands</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1849</td>
<td></td>
</tr>
<tr>
<td>debug epsr</td>
<td>1849</td>
<td></td>
</tr>
<tr>
<td>epsr</td>
<td>1850</td>
<td></td>
</tr>
<tr>
<td>epsr configuration</td>
<td>1851</td>
<td></td>
</tr>
<tr>
<td>epsr datavlan</td>
<td>1853</td>
<td></td>
</tr>
<tr>
<td>epsr enhancedrecovery enable</td>
<td>1855</td>
<td></td>
</tr>
<tr>
<td>epsr mode master controlvlan primary port</td>
<td>1856</td>
<td></td>
</tr>
<tr>
<td>epsr mode transit controlvlan</td>
<td>1857</td>
<td></td>
</tr>
<tr>
<td>epsr priority</td>
<td>1858</td>
<td></td>
</tr>
<tr>
<td>epsr state</td>
<td>1859</td>
<td></td>
</tr>
<tr>
<td>epsr trap</td>
<td>1860</td>
<td></td>
</tr>
<tr>
<td>show debugging epsr</td>
<td>1861</td>
<td></td>
</tr>
<tr>
<td>show epsr</td>
<td>1862</td>
<td></td>
</tr>
<tr>
<td>show epsr common segments</td>
<td>1867</td>
<td></td>
</tr>
<tr>
<td>show epsr config-check</td>
<td>1868</td>
<td></td>
</tr>
<tr>
<td>show epsr &lt;epsr-instance&gt;</td>
<td>1870</td>
<td></td>
</tr>
<tr>
<td>show epsr &lt;epsr-instance&gt; counters</td>
<td>1871</td>
<td></td>
</tr>
<tr>
<td>show epsr counters</td>
<td>1872</td>
<td></td>
</tr>
<tr>
<td>show epsr summary</td>
<td>1873</td>
<td></td>
</tr>
<tr>
<td>undebug epsr</td>
<td>1874</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 45:</th>
<th>AMF Commands</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1875</td>
<td></td>
</tr>
<tr>
<td>atmf area</td>
<td>1876</td>
<td></td>
</tr>
<tr>
<td>atmf area password</td>
<td>1877</td>
<td></td>
</tr>
<tr>
<td>atmf backup</td>
<td>1879</td>
<td></td>
</tr>
<tr>
<td>atmf backup area-masters delete</td>
<td>1880</td>
<td></td>
</tr>
<tr>
<td>atmf backup area-masters enable</td>
<td>1881</td>
<td></td>
</tr>
<tr>
<td>atmf backup area-masters now</td>
<td>1882</td>
<td></td>
</tr>
<tr>
<td>atmf backup area-masters synchronize</td>
<td>1883</td>
<td></td>
</tr>
<tr>
<td>atmf backup bandwidth</td>
<td>1884</td>
<td></td>
</tr>
<tr>
<td>atmf backup delete</td>
<td>1885</td>
<td></td>
</tr>
<tr>
<td>atmf backup enable</td>
<td>1886</td>
<td></td>
</tr>
<tr>
<td>atmf backup now</td>
<td>1887</td>
<td></td>
</tr>
<tr>
<td>atmf backup server</td>
<td>1889</td>
<td></td>
</tr>
<tr>
<td>atmf backup stop</td>
<td>1891</td>
<td></td>
</tr>
<tr>
<td>atmf backup synchronize</td>
<td>1892</td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 46: NTP Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2002</td>
</tr>
<tr>
<td>ntp access-group</td>
<td>2003</td>
</tr>
<tr>
<td>ntp authenticate</td>
<td>2004</td>
</tr>
<tr>
<td>ntp authentication-key</td>
<td>2005</td>
</tr>
<tr>
<td>ntp broadcastdelay</td>
<td>2006</td>
</tr>
<tr>
<td>ntp master</td>
<td>2007</td>
</tr>
<tr>
<td>ntp peer</td>
<td>2008</td>
</tr>
<tr>
<td>ntp server</td>
<td>2010</td>
</tr>
<tr>
<td>ntp source</td>
<td>2012</td>
</tr>
<tr>
<td>ntp trusted-key</td>
<td>2014</td>
</tr>
<tr>
<td>show counter ntp</td>
<td>2015</td>
</tr>
<tr>
<td>show ntp associations</td>
<td>2017</td>
</tr>
<tr>
<td>show ntp status</td>
<td>2019</td>
</tr>
</tbody>
</table>

### Chapter 47: Dynamic Host Configuration Protocol (DHCP) Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2020</td>
</tr>
<tr>
<td>bootfile</td>
<td>2021</td>
</tr>
<tr>
<td>clear ip dhcp binding</td>
<td>2022</td>
</tr>
<tr>
<td>default-router</td>
<td>2023</td>
</tr>
<tr>
<td>dns-server</td>
<td>2024</td>
</tr>
<tr>
<td>domain-name</td>
<td>2025</td>
</tr>
<tr>
<td>host</td>
<td>2026</td>
</tr>
<tr>
<td>ip address dhcp</td>
<td>2027</td>
</tr>
<tr>
<td>ip dhcp bootp ignore</td>
<td>2029</td>
</tr>
<tr>
<td>ip dhcp leasequery enable</td>
<td>2030</td>
</tr>
<tr>
<td>ip dhcp option</td>
<td>2031</td>
</tr>
<tr>
<td>ip dhcp pool</td>
<td>2033</td>
</tr>
<tr>
<td>ip dhcp-relay agent-option</td>
<td>2034</td>
</tr>
<tr>
<td>ip dhcp-relay agent-option checking</td>
<td>2036</td>
</tr>
<tr>
<td>ip dhcp-relay agent-option remote-id</td>
<td>2037</td>
</tr>
<tr>
<td>ip dhcp-relay information policy</td>
<td>2038</td>
</tr>
<tr>
<td>ip dhcp-relay maxhops</td>
<td>2040</td>
</tr>
<tr>
<td>ip dhcp-relay max-message-length</td>
<td>2041</td>
</tr>
<tr>
<td>ip dhcp-relay server-address</td>
<td>2043</td>
</tr>
<tr>
<td>lease</td>
<td>2045</td>
</tr>
<tr>
<td>network (DHCP)</td>
<td>2047</td>
</tr>
<tr>
<td>next-server</td>
<td>2048</td>
</tr>
<tr>
<td>option</td>
<td>2049</td>
</tr>
<tr>
<td>probe enable</td>
<td>2051</td>
</tr>
<tr>
<td>probe packets</td>
<td>2052</td>
</tr>
<tr>
<td>probe timeout</td>
<td>2053</td>
</tr>
<tr>
<td>probe type</td>
<td>2054</td>
</tr>
<tr>
<td>range</td>
<td>2055</td>
</tr>
<tr>
<td>route</td>
<td>2056</td>
</tr>
<tr>
<td>service dhcp-relay</td>
<td>2057</td>
</tr>
<tr>
<td>service dhcp-server</td>
<td>2058</td>
</tr>
</tbody>
</table>
show counter dhcp-client .......................... 2059
show counter dhcp-relay .......................... 2060
show counter dhcp-server .......................... 2063
show dhcp lease ................................. 2065
show ip dhcp binding .............................. 2067
show ip dhcp pool ................................. 2069
show ip dhcp-relay ............................... 2073
show ip dhcp server statistics ....................... 2074
show ip dhcp server summary ....................... 2076
subnet-mask ........................................ 2077

Chapter 48: DHCP for IPv6 (DHCPv6) Commands ................. 2078

Introduction ........................................ 2078
address prefix .................................... 2079
address range ..................................... 2081
clear counter ipv6 dhcp-client ....................... 2083
clear counter ipv6 dhcp-server ....................... 2084
clear ipv6 dhcp binding ............................. 2085
clear ipv6 dhcp client .............................. 2087
dns-server (DHCPv6) ............................... 2088
domain-name (DHCPv6) ............................. 2090
ip dhcp-relay agent-option subscriber-id-auto-mac ............. 2091
ipv6 address (DHCPv6 PD) .......................... 2092
ipv6 address dhcp ................................ 2095
ipv6 dhcp client pd ............................... 2097
ipv6 dhcp option ................................... 2099
ipv6 dhcp pool .................................... 2101
ipv6 dhcp server .................................. 2103
ipv6 local pool ................................... 2104
ipv6 nd prefix (DHCPv6) .......................... 2106
link-address ....................................... 2108
option (DHCPv6) ................................... 2110
prefix-delegation pool .............................. 2112
show counter ipv6 dhcp-client ....................... 2114
show counter ipv6 dhcp-server ....................... 2116
show ipv6 dhcp ................................... 2118
show ipv6 dhcp binding ............................. 2119
show ipv6 dhcp interface .......................... 2122
show ipv6 dhcp pool ............................... 2124
snntp-address .................................... 2126

Chapter 49: SNMP Commands .................................. 2127

Introduction ........................................ 2127
debug snmp ....................................... 2128
show counter snmp-server ........................... 2129
show debugging snmp ................................ 2133
show running-config snmp ............................ 2134
show snmp-server ................................. 2135
show snmp-server community ....................... 2136
show snmp-server group ............................. 2137
show snmp-server user .............................. 2138
show snmp-server view ............................. 2139
Chapter 50: LLDP Commands ................................. 2166

Introduction ................................................. 2166

- clear lldp statistics ................................. 2167
- clear lldp table .................................... 2168
- debug lldp ............................................. 2169
- lldp faststart-count .............................. 2171
- lldp holdtime-multiplier ....................... 2172
- lldp management-address ..................... 2173
- lldp med-notifications .......................... 2174
- lldp med-tlv-select .............................. 2175
- lldp non-strict-med-tlv-order-check ....... 2177
- lldp notification-interval .................... 2178
- lldp notifications .................................. 2179
- lldp port-number-type ............................ 2180
- lldp reinit ........................................... 2181
- lldp run .............................................. 2182
- lldp timer ........................................... 2183
- lldp tlv-select ..................................... 2184
- lldp transmit receive .......................... 2186
- lldp tx-delay ...................................... 2187
- location civic-location configuration ...... 2188
- location civic-location identifier .......... 2193
- location civic-location-id ...................... 2194
- location coord-location configuration ...... 2195
- location coord-location identifier .......... 2197
- location coord-location-id ................... 2198
- location elin-location ......................... 2199
- location elin-location-id ..................... 2200
- show debugging lldp ............................ 2201
- show lldp ............................................ 2203
- show lldp interface ............................. 2205
- show lldp local-info ............................. 2207
- show lldp neighbors ............................. 2212
- show lldp neighbors detail .................... 2214
- show lldp statistics ............................. 2218
- show lldp statistics interface .............. 2220
Chapter 51: **SMTP Commands** ........................................ 2244

Introduction ................................................................. 2244

done mail ............................................................... 2225
delete mail ............................................................... 2226
mail ................................................................. 2227
mail from ............................................................... 2228
mail smtpserver ......................................................... 2229
show counter mail ...................................................... 2230
show mail ............................................................... 2231
undebug mail ............................................................ 2232

Chapter 52: **RMON Commands** ........................................ 2233

Introduction ................................................................. 2233

rmon alarm ............................................................... 2234
rmon collection history .............................................. 2236
rmon collection stats .................................................. 2237
rmon event ............................................................... 2238
show rmon alarm .......................................................... 2239
show rmon event .......................................................... 2240
show rmon history ....................................................... 2242
show rmon statistics .................................................... 2244

Chapter 53: **Trigger Commands** ........................................ 2246

Introduction ................................................................. 2246

active (trigger) .......................................................... 2247
day ................................................................. 2248
debug trigger ............................................................ 2250
description (trigger) .................................................... 2251
repeat ................................................................. 2252
script ................................................................. 2253
show debugging trigger ................................................. 2255
show running-config trigger ............................................ 2256
show trigger ............................................................. 2257
test ................................................................. 2262
time (trigger) ............................................................ 2263
trap ................................................................. 2265
trigger ................................................................. 2266
trigger activate .......................................................... 2267
type atmf node .......................................................... 2268
type cpu ............................................................... 2271
type interface ........................................................... 2272
type memory ............................................................. 2273
type periodic ............................................................ 2274
type ping-poll ............................................................ 2275
type reboot ............................................................... 2276
type stack disabled-master ............................................. 2277
type stack link ........................................................... 2278
type stack master-fail .................................................... 2279
type stack member ........................................................ 2280
type time ............................................................... 2281

show location ........................................................... 2222
<table>
<thead>
<tr>
<th>Chapter 54:</th>
<th>Ping-Polling Commands</th>
<th>2284</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2284</td>
<td></td>
</tr>
<tr>
<td>active (ping-polling)</td>
<td>2285</td>
<td></td>
</tr>
<tr>
<td>clear ping-poll</td>
<td>2286</td>
<td></td>
</tr>
<tr>
<td>critical-interval</td>
<td>2287</td>
<td></td>
</tr>
<tr>
<td>debug ping-poll</td>
<td>2288</td>
<td></td>
</tr>
<tr>
<td>description (ping-polling)</td>
<td>2289</td>
<td></td>
</tr>
<tr>
<td>fail-count</td>
<td>2290</td>
<td></td>
</tr>
<tr>
<td>ip (ping-polling)</td>
<td>2291</td>
<td></td>
</tr>
<tr>
<td>length (ping-poll data)</td>
<td>2292</td>
<td></td>
</tr>
<tr>
<td>normal-interval</td>
<td>2293</td>
<td></td>
</tr>
<tr>
<td>ping-poll</td>
<td>2294</td>
<td></td>
</tr>
<tr>
<td>sample-size</td>
<td>2295</td>
<td></td>
</tr>
<tr>
<td>show counter ping-poll</td>
<td>2297</td>
<td></td>
</tr>
<tr>
<td>show ping-poll</td>
<td>2299</td>
<td></td>
</tr>
<tr>
<td>source-ip</td>
<td>2303</td>
<td></td>
</tr>
<tr>
<td>timeout (ping polling)</td>
<td>2304</td>
<td></td>
</tr>
<tr>
<td>up-count</td>
<td>2305</td>
<td></td>
</tr>
<tr>
<td>unddebug ping-poll</td>
<td>2306</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 55:</th>
<th>sFlow Commands</th>
<th>2307</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2307</td>
<td></td>
</tr>
<tr>
<td>debug sflow</td>
<td>2308</td>
<td></td>
</tr>
<tr>
<td>debug sflow agent</td>
<td>2309</td>
<td></td>
</tr>
<tr>
<td>sflow agent (address)</td>
<td>2310</td>
<td></td>
</tr>
<tr>
<td>sflow collector (address)</td>
<td>2312</td>
<td></td>
</tr>
<tr>
<td>sflow collector max-datagram-size</td>
<td>2314</td>
<td></td>
</tr>
<tr>
<td>sflow enable</td>
<td>2315</td>
<td></td>
</tr>
<tr>
<td>sflow max-header-size</td>
<td>2316</td>
<td></td>
</tr>
<tr>
<td>sflow polling-interval</td>
<td>2318</td>
<td></td>
</tr>
<tr>
<td>sflow sampling-rate</td>
<td>2319</td>
<td></td>
</tr>
<tr>
<td>show debugging sflow</td>
<td>2320</td>
<td></td>
</tr>
<tr>
<td>show running-config sflow</td>
<td>2322</td>
<td></td>
</tr>
<tr>
<td>show sflow</td>
<td>2323</td>
<td></td>
</tr>
<tr>
<td>show sflow interface</td>
<td>2325</td>
<td></td>
</tr>
<tr>
<td>unddebug sflow</td>
<td>2326</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 56:</th>
<th>Cable Fault Locator Commands</th>
<th>2327</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2327</td>
<td></td>
</tr>
<tr>
<td>clear test cable-diagnostics tdr</td>
<td>2328</td>
<td></td>
</tr>
<tr>
<td>show test cable-diagnostics tdr</td>
<td>2329</td>
<td></td>
</tr>
<tr>
<td>test cable-diagnostics tdr interface</td>
<td>2330</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 57:</th>
<th>Stacking Commands</th>
<th>2331</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2331</td>
<td></td>
</tr>
<tr>
<td>clear counter stack</td>
<td>2333</td>
<td></td>
</tr>
<tr>
<td>debug stack</td>
<td>2334</td>
<td></td>
</tr>
<tr>
<td>reboot rolling</td>
<td>2335</td>
<td></td>
</tr>
<tr>
<td>reload rolling</td>
<td>2336</td>
<td></td>
</tr>
</tbody>
</table>
remote-command (deleted) ........................................... 2337
remote-login ......................................................... 2338
show counter stack ................................................. 2339
show debugging stack .............................................. 2343
show running-config stack ........................................ 2344
show provisioning (stack) .......................................... 2345
show stack .......................................................... 2346
show stack resiliencylink .......................................... 2352
stack disabled-master-monitoring ................................. 2354
stack enable ........................................................ 2355
stack management subnet ......................................... 2357
stack management vlan ........................................... 2358
stack priority ....................................................... 2359
stack renumber ...................................................... 2360
stack renumber cascade ........................................... 2361
stack resiliencylink ............................................... 2363
stack software-auto-synchronize ................................ 2365
stack virtual-chassis-id ......................................... 2366
stack virtual-mac .................................................. 2367
switch provision (stack) ......................................... 2368
switchport resiliencylink ......................................... 2369
vlan mode stack-local-vlan ....................................... 2370
undebug stack ...................................................... 2371
List of Commands

(access-list extended ICMP filter) 1345
(access-list extended IP filter) 1347
(access-list extended IP protocol filter) 1350
(access-list extended TCP UDP filter) 1355
(access-list hardware ICMP filter) 1314
(access-list hardware IP protocol filter) 1317
(access-list hardware MAC filter) 1323
(access-list hardware TCP UDP filter) 1326
(access-list standard named filter) 1362
(access-list standard numbered filter) 1364
(ipv6 access-list extended IP protocol filter) 1410
(ipv6 access-list extended TCP UDP filter) 1413
(ipv6 access-list named ICMP filter) 1385
(ipv6 access-list named protocol filter) 1388
(ipv6 access-list named TCP UDP filter) 1393
(ipv6 access-list standard filter) 1417
aaa accounting auth-mac default 1616
aaa accounting auth-web default 1618
aaa accounting commands 1620
aaa accounting dot1x 1622
aaa accounting login 1624
aaa accounting update 1627
aaa authentication auth-mac 1629
aaa authentication auth-web 1630
aaa authentication dot1x 1631
aaa authentication enable default group tacacs+ 1632
aaa authentication enable default local 1634
aaa authentication login 1635
aaa group server 1637
aaa local authentication attempts lockout-time 1639
aaa local authentication attempts max-fail 1640
abr-type 921
accept-lifetime 739
access-group 1297
access-list (extended numbered) 1343
access-list (hardware IP numbered) 1299
access-list (hardware MAC numbered) 1309
access-list (standard numbered) 1360
access-list extended (named) 1335
access-list hardware (named) 1312
access-list standard (named) 1358
accounting login 1641
activate 352
active (ping-polling) 2285
active (trigger) 2247
address prefix 2079
address range 2081
advertisement-interval 1813
aggregate-address (IPv6 RIPng) 792
alliedware-behavior 741
area authentication 818
area authentication ipsec spi 922
area default-cost (IPv6 OSPF) 924
area default-cost 817
area encryption ipsec spi esp 925
area filter-list 819
area nssa 820
area range (IPv6 OSPF) 928
area range 822
area stub (IPv6 OSPF) 930
area stub 824
area virtual-link (IPv6 OSPF) 931
area virtual-link 825
area virtual-link authentication ipsec spi 933
area virtual-link encryption ipsec spi 935
arp (IP address MAC) 636
arp log 637
arp opportunistic-nd 640
arp security 1764
arp security violation 1765
arp-aging-timeout 634
arp-mac-disparity 635
atmf area 1876
atmf area password 1877
atmf backup 1879
atmf backup area-masters delete 1880
atmf backup area-masters enable 1881
atmf backup area-masters now 1882
atmf backup area-masters synchronize 1883
atmf backup bandwidth 1884
atmf backup delete 1885
atmf backup enable 1886
atmf backup now 1887
atmf backup server 1889
atmf backup stop 1891
atmf backup synchronize 1892
atmf cleanup 1893
atmf controller 1894
atmf distribute firmware 1895
atmf domain vlan 1897
atmf enable 1899
atmf group (membership) 1900
atmf log-verbose 1902
atmf management subnet 1903
atmf management vlan 1905
atmf master 1907
atmf network-name 1908
atmf provision 1909
atmf provision node clone 1910
atmf provision node configure boot config 1912
atmf provision node configure boot system 1914
atmf provision node create 1916
atmf provision node delete 1918
atmf provision node license-cert 1920
atmf provision node locate 1922
atmf reboot-rolling 1923
atmf recover 1927
atmf recover led-off 1929
atmf remote-login 1930
atmf restricted-login 1931
atmf select-area 1932
atmf virtual-link 1933
atmf working-set 1936
attribute 1669
auth auth-fail vlan 1517
auth critical 1519
auth dynamic-vlan-creation 1520
auth guest-vlan 1523
auth host-mode 1525
auth log 1527
auth max-suppliant 1529
auth reauthentication 1530
auth roaming disconnected 1531
auth roaming enable 1533
auth supplicant-mac 1535
auth timeout connect-timeout 1537
auth timeout quiet-period 1538
auth timeout reauth-period 1539
auth timeout server-timeout 1540
auth timeout supp-timeout 1541
auth two-step enable 1542
authentication 1672
auth-mac enable 1545
auth-mac method 1547
auth-mac password 1548
auth-mac reauth-relearning 1550
auth-web enable 1551
auth-web forward 1552
auth-web max-auth-fail 1554
auth-web method 1555
auth-web-server blocking-mode 1556
auth-web-server dhcp ipaddress 1557
auth-web-server dhcp lease 1558
auth-web-server dhcp-wpad-option 1559
auth-web-server gateway (deleted) 1560
auth-web-server host-name 1561
auth-web-server http-redirect (deleted) 1562
auth-web-server intercept-port 1563
auth-web-server ipaddress 1564
auth-web-server login-url 1565
auth-web-server mode (deleted) 1566
auth-web-server page logo 1567
auth-web-server page sub-title 1568
auth-web-server page success-message 1569
auth-web-server page title 1570
auth-web-server page welcome-message 1571
auth-web-server ping-poll enable 1572
auth-web-server ping-poll failcount 1573
auth-web-server ping-poll interval 1574
auth-web-server ping-poll reauth-timer-refresh 1575
auth-web-server ping-poll timeout 1576
auth-web-server port 1577
auth-web-server redirect-delay-time 1578
auth-web-server redirect-url 1579
auth-web-server session-keep 1580
auth-web-server ssl 1581
auth-web-server ssl intercept-port 1583
auth-web-server ss1port (deleted) 1582
autoboot enable 136
auto-cost reference bandwidth (IPv6 OSPF) 938
auto-cost reference bandwidth 828
backpressure 379
bandwidth (duplicate) 940
bandwidth 830
banner exec 216
banner login (SSH) 1718
banner login (system) 218
banner motd 220
boot config-file 137
boot config-file backup 139
boot system 140
boot system backup 142
bootfile 2021
capability opaque 831
capability restart 832
cd 143
channel-group 572
circuit-failover 1815
cisco-metric-behavior (RIP) 743
class 1424
class-map 1425
clear aaa local user lockout 1642
clear arp security statistics 1767
clear arp-cache 641
clear atmf links statistics 1938
clear counter ipv6 dhcp-client 2083
clear counter ipv6 dhcp-server 2084
clear counter stack 2333
clear exception log 297
clear gvrp statistics 619
clear ip dhcp binding 2022
clear ip dhcp snooping binding 1768
clear ip dhcp snooping statistics 1769
clear ip dns forwarding cache 642
clear ip igmp 1069
clear ip igmp group 1070
clear ip igmp interface 1071
clear ip mroute 1041
clear ip mroute pim sparse-mode 1158
clear ip mroute statistics 1042
clear ip ospf process 833
clear ip pim sparse-mode bsr rp-set * 1157
clear ip prefix-list 1366
clear ip rip route 744
clear ipv6 dhcp binding 2085
clear ipv6 dhcp client 2087
clear ipv6 mld 1123
clear ipv6 mld group 1124
clear ipv6 mld interface 1125
clear ipv6 mroute 1043
clear ipv6 mroute pim 1207
clear ipv6 mroute pim sparse-mode 1208
clear ipv6 mroute statistics 1044
clear ipv6 neighbors 697
clear ipv6 ospf process 941
clear ipv6 pim sparse-mode bsr rp-set * 1209
clear ipv6 rip route 793
clear lacp counters 574
clear line console 94
clear line vty 95
clear lldp statistics 2167
clear lldp table 2168
clear log 298
clear log buffered 299
clear log permanent 300
clear loop-protection counters 381
clear mac address-table dynamic 383
clear mac address-table static 382
clear mls qos interface policer-counters 1426
clear ping-poll 2286
clear port counter 385
clear power-inline counters interface 595
clear radius local-server statistics 1673
clear spanning-tree detected protocols (RSTP and MSTP) 495
clear spanning-tree statistics 494
clear ssh 1719
clear test cable-diagnostics tdr 2328
clear test interface 374
clear vlan statistics 445
clock set 222
clock summer-time date 223
clock summer-time recurring 225
clock timezone 227
commit (IPv4) 1329
commit (IPv6) 1382
compatible rfc1583 834
configure terminal 83
continuous-reboot-prevention 228
copy (filename) 148
copy current-software 144
copy debug 145
copy fdb-radius-users (to file) 1674
copy local-radius-user-db (from file) 1676
copy local-radius-user-db (to file) 1677
copy proxy-autoconfig-file 1584
copy running-config 146
copy startup-config 147
copy web-auth-https-file 1585
copy zmodem 150
create autoboot 151
critical-interval 2287
crypto key destroy hostkey 1720
crypto key destroy userkey 1721
crypto key generate hostkey 1722
crypto key generate userkey 1723
crypto key pubkey-chain knownhosts 1724
crypto key pubkey-chain userkey 1726
crypto pki enroll local 1678
crypto pki enroll local local-radius-all-users 1679
crypto pki enroll local user 1680
crypto pki export local pem 1681
crypto pki export local pkcs12 1682
crypto pki trustpoint local 1683
day 2248
deadtime (RADIUS server group) 1649
debug aaa 1643
debug arp security 1770
debug atm 1939
debug atm packet 1941
debug crypto pki 1684
debug dot1x 1483
debug epsr 1850
debug gvrp 620
debug igmp 1072
debug ip dhcp snooping 1771
debug ip dns forwarding 643
debug ip packet interface 644
debug ipv6 ospf events 942
debug ipv6 ospf ifsm 943
debug ipv6 ospf lsa 944
debug ipv6 ospf nfsm 945
debug ipv6 ospf packet 946
debug ipv6 ospf route 947
debug ipv6 pim sparse-mode 1210
debug ipv6 pim sparse-mode packet 1212
debug ipv6 pim sparse-mode timer 1213
debug ipv6 rip 794
debug lacp 575
debug lldp 2169
debug loopprot 386
debug mail 2225
debug mld 1126
debug mstp (RSTP and STP) 496
debug nsm mcast 1045
debug nsm mcast6 1046
d debug ospf events 835
d debug ospf ifsm 836
d debug ospf isa 837
d debug ospf nfsm 838
d debug ospf nsm 839
d debug ospf packet 840
d debug ospf route 841
d debug pim dense-mode all 1267
d debug pim dense-mode context 1268
d debug pim dense-mode decode 1269
d debug pim dense-mode encode 1270
d debug pim dense-mode fsm 1271
d debug pim dense-mode mrt 1272
d debug pim dense-mode nexthop 1273
d debug pim dense-mode nsm 1274
d debug pim dense-mode vif 1275
d debug pim sparse-mode 1159
d debug pim sparse-mode timer 1160
d debug ping-poll 2288
d debug platform packet 387
d debug power-inline 596
d debug radius 1650
d debug rip 745
d debug sflow 2308
d debug sflow agent 2309
debug snmp 2128
default log buffered 301
default log console 302
default log email 303
default log host 304
default log permanent 306
default-action 1427
default-information originate (IPv6 RIPng) 795
default-information originate (OSPF) 842
default-information originate (RIP) 746
default-metric (IPv6 OSPF) 948
default-metric (IPv6 RIPng) 796
default-metric (OSPF) 843
default-metric (RIP) 747
default-router 2023
delete 152
delete debug 153
delete mail 2226
description (interface) 356
description (ping-polling) 2289
description (QoS policy-map) 1428
description (trigger) 2251
dir 154
disable (Privileged Exec mode) 84
disable (VRRP) 1820
distance (IPv6 OSPF) 949
distance (OSPF) 844
distance (RIP) 748

distribute-list (IPv6 OSPF) 951
distribute-list (IPv6 RIPng) 797
distribute-list (OSPF) 846
distribute-list (RIP) 749
dns-server (DHCPv6) 2088
dns-server 2024
do 85
domain-name (DHCPv6) 2090
domain-name 2025
domain-style 1685
dos 1367
dot1x control-direction 1484
dot1x eap 1485
dot1x eapol-version 1486
dot1x initialize interface 1487
dot1x initialize supplicant 1488
dot1x keytransmit 1489
dot1x max-auth-fail 1490
dot1x max-reauth-req 1492
dot1x port-control 1493
dot1x timeout tx-period 1495
duplex 389
echo 353
ecofriendly led 230
ecofriendly lpi 231
edit (filename) 157
edit 156
egress-rate-limit 1429
egress-vlan-id 1686
egress-vlan-name 1688
enable (Privileged Exec mode) 86
enable (VRRP) 1821
enable db-summary-opt 848
enable password 96
enable secret 99
end 88
epsr 1851
epsr configuration 1853
epsr datavlan 1854
epsr enhancedrecovery enable 1855
epsr mode master controlvlan primary port 1856
epsr mode transit controlvlan 1857
epsr priority 1858
epsr state 1859
epsr trap 1860
erase factory-default 1944
erase proxy-autoconfig-file 1586
erase startup-config 159
erase web-auth-https-file 1587
exception coredump size (deleted) 307
exec-timeout 102
exit 89
fail-count 2290
findme 233
flowcontrol (switch port) 390
flowcontrol hardware (asyn/console) 104
fullupdate (RIP) 750
group 1690
gvrp (interface) 622
gvrp dynamic-vlan-creation 623
gvrp enable (global) 624
gvrp registration 625
gvrp timer 626
help 90
host 2026
host area 849
hostname 235
instance priority (MSTP) 500
instance vlan (MSTP) 502
interface (to configure) 357
ip (ping-polling) 2291
ip address 646
ip address dhcp 2027
ip dhcp bootp ignore 2029
ip dhcp leasequery enable 2030
ip dhcp option 2031
ip dhcp pool 2033
ip dhcp snooping 1772
ip dhcp snooping agent-option 1773
ip dhcp snooping agent-option allow-untrusted 1774
ip dhcp snooping agent-option circuit-id vlantriplet 1775
ip dhcp snooping agent-option remote-id 1776
ip dhcp snooping binding 1777
ip dhcp snooping database 1778
ip dhcp snooping delete-by-client 1779
ip dhcp snooping delete-by-linkdown 1780
ip dhcp snooping max-bindings 1781
ip dhcp snooping subscriber-id 1782
ip dhcp snooping trust 1783
ip dhcp snooping verify mac-address 1784
ip dhcp snooping violation 1785
ip dhcp-relay agent-option 2034
ip dhcp-relay agent-option checking 2036
ip dhcp-relay agent-option remote-id 2037
ip dhcp-relay agent-option subscriber-id-auto-mac 2091
ip dhcp-relay information policy 2038
ip dhcp-relay maxhops 2040
ip dhcp-relay max-message-length 2041
ip dhcp-relay server-address 2043
ip directed-broadcast 648
ip dns forwarding 650
ip dns forwarding cache 651
ip dns forwarding dead-time 652
ip dns forwarding retry 653
ip dns forwarding source-interface 654
ip dns forwarding timeout 655
ip domain-list 656
ip domain-lookup 657
ip domain-name 658
ip forward-protocol udp 659
ip gratuitous-arp-link 661
ip helper-address 663
ip igmp 1073
ip igmp access-group 1074
ip igmp immediate-leave 1075
ip igmp last-member-query-count 1076
ip igmp last-member-query-interval 1077
ip igmp limit 1078
ip igmp mroute-proxy 1080
ip igmp proxy-service 1081
ip igmp querier-timeout 1082
ip igmp query-holdtime 1083
ip igmp query-interval 1085
ip igmp query-max-response-time 1087
ip igmp ra-option (Router Alert) 1089
ip igmp robustness-variable 1090
ip igmp snooping 1091
ip igmp snooping fast-leave 1092
ip igmp snooping mrouter 1093
ip igmp snooping querier 1094
ip igmp snooping report-suppression 1095
ip igmp snooping routermode 1096
ip igmp snooping tcn query solicit 1098
ip igmp source-address-check 1100
ip igmp ssm 1101
ip igmp ssm-map enable 1102
ip igmp ssm-map static 1103
ip igmp startup-query-count 1107
ip igmp startup-query-interval 1108
ip igmp static-group 1105
ip igmp version 1109
ip local-proxy-arp 665
ip mroute 1047
ip multicast forward-first-packet 1049
ip multicast route 1050
ip multicast route-limit 1052
ip multicast wrong-vif-suppression 1053
ip multicast-routing 1054
ip name-server 666
ip ospf authentication 850
ip ospf authentication-key 851
ip ospf cost 852
ip ospf database-filter 853
ip ospf dead-interval 854
ip ospf disable all 855
ip ospf hello-interval 856
ip ospf message-digest-key 857
ip ospf mtu 859
ip ospf mtu-ignore 860
ip ospf network 861
ip ospf priority 862
ip ospf resync-timeout 863
ip ospf retransmit-interval 864
ip ospf transmit-delay 865
ip pim accept-register list 1162
ip pim anycast-rp 1163
ip pim bsr-border 1164
ip pim bsr-candidate 1165
ip pim cisco-register-checksum 1166
ip pim cisco-register-checksum group-list 1167
ip pim crp-cisco-prefix 1168
ip pim dense-mode 1276
ip pim dense-mode passive 1277
ip pim dr-priority 1169
ip pim exclude-genid 1170
ip pim ext-srcs-directly-connected (PIM-DM) 1278
ip pim ext-srcs-directly-connected (PIM-SM) 1171
ip pim hello-holdtime (PIM-DM) 1279
ip pim hello-holdtime (PIM-SM) 1172
ip pim hello-interval (PIM-DM) 1280
ip pim hello-interval (PIM-SM) 1173
ip pim ignore-rp-set-priority 1174
ip pim jp-timer 1175
ip pim max-graft-retries 1281
ip pim neighbor-filter (PIM-DM) 1283
ip pim neighbor-filter (PIM-SM) 1176
ip pim propagation-delay 1284
ip pim register-rate-limit 1177
ip pim register-rp-reachability 1178
ip pim register-source 1179
ip pim register-suppression 1180
ip pim rp-address 1181
ip pim rp-candidate 1183
ip pim rp-register-kat 1184
ip pim sparse-mode 1185
ip pim sparse-mode passive 1186
ip pim spt-threshold 1187
ip pim spt-threshold group-list 1188
ip pim ssm 1189
ip pim state-refresh origination-interval 1285
ip prefix-list 1370
ip proxy-arp 667
ip radius source-interface 1651
ip redirects 668
ip rip authentication key-chain 751
ip rip authentication mode 753
ip rip authentication string 756
ip rip receive version 759
ip rip receive-packet 758
ip rip send version 1-compatible 763
ip rip send version 761
ip rip send-packet 760
ip rip split-horizon 765
ip route 729
ip source binding 1786
ipv6 access-list (named) 1383
ipv6 access-list extended (named) 1403
ipv6 access-list extended proto 1407
ipv6 access-list standard (named) 1415
ipv6 address (DHCPv6 PD) 2092
ipv6 address 698
ipv6 address autoconfig 700
ipv6 address dhcp 2095
ipv6 dhcp client pd 2097
ipv6 dhcp option 2099
ipv6 dhcp pool 2101
ipv6 dhcp server 2103
ipv6 enable 702
ipv6 forwarding 704
ipv6 local pool 2104
ipv6 mld 1129
ipv6 mld access-group 1130
ipv6 mld immediate-leave 1131
ipv6 mld last-member-query-count 1132
ipv6 mld last-member-query-interval 1133
ipv6 mld limit 1134
ipv6 mld querier-timeout 1136
ipv6 mld query-interval 1137
ipv6 mld query-max-response-time 1138
ipv6 mld robustness-variable 1139
ipv6 mld snooping 1140
ipv6 mld snooping fast-leave 1142
ipv6 mld snooping mrouting 1143
ipv6 mld snooping querier 1145
ipv6 mld snooping report-suppression 1146
ipv6 mld static-group 1148
ipv6 mld version 1150
ipv6 multicast route 1055
ipv6 multicast route-limit 1058
ipv6 multicast-routing 1059
ipv6 nd managed-config-flag 705
ipv6 nd minimum-ra-interval 706
ipv6 nd other-config-flag 707
ipv6 nd prefix (DHCPv6) 2106
ipv6 nd prefix 708
ipv6 nd raguard 712
ipv6 nd ra-interval 710
ipv6 nd ra-lifetime 711
ipv6 nd reachable-time 714
ipv6 nd retransmission-time 715
ipv6 nd suppress-ra 716
ipv6 neighbor 717
ipv6 opportunistic-nd 718
ipv6 ospf authentication spi 953
ipv6 ospf cost 955
ipv6 ospf dead-interval 956
ipv6 ospf display route single-line 957
ipv6 ospf encryption spi esp 958
ipv6 ospf hello-interval 961
ipv6 ospf network 962
ipv6 ospf priority 963
ipv6 ospf retransmit-interval 964
ipv6 ospf transmit-delay 965
ipv6 pim accept-register 1215
ipv6 pim anycast-rp 1216
ipv6 pim bsr-border 1217
ipv6 pim bsr-candidate 1218
ipv6 pim cisco-register-checksum 1219
ipv6 pim cisco-register-checksum group-list 1220
ipv6 pim crp-cisco-prefix 1221
ipv6 pim dr-priority 1222
ipv6 pim exclude-genid 1223
ipv6 pim ext-srscs-directly-connected 1224
ipv6 pim hello-holdtime 1225
ipv6 pim hello-interval 1226
ipv6 pim ignore-rp-set-priority 1227
ipv6 pim jp-timer 1228
ipv6 pim neighbor-filter 1229
ipv6 pim register-rate-limit 1230
ipv6 pim register-rp-reachability 1231
ipv6 pim register-source 1232
ipv6 pim register-suppression 1233
ipv6 pim rp embedded 1238
ipv6 pim rp-address 1234
ipv6 pim rp-candidate 1236
ipv6 pim rp-register-kat 1239
ipv6 pim sparse-mode 1240
ipv6 pim sparse-mode passive 1241
ipv6 pim spt-threshold 1242
ipv6 pim spt-threshold group-list 1243
ipv6 pim ssm 1244
ipv6 pim unicast-bsm 1245
ipv6 prefix-list 1419
ipv6 rip metric-offset 798
ipv6 rip split-horizon 800
ipv6 route 719
ipv6 router ospf area 966
ipv6 router rip 801
ipv6 traffic-filter 1397
key 766
key chain 767
key-string 768
lacp port-priority 576
lacp system-priority 577
lacp timeout 578
lease 2045
length (asyn) 106
length (ping-poll data) 2292
license 204
license member (deleted) 206
line 107
link-address 2108
linkflap action 392
lldp faststart-count 2171
lldp holdtime-multiplier 2172
lldp management-address 2173
lldp med-notifications 2174
lldp med-tlv-select 2175
lldp non-strict-med-tlv-order-check 2177
lldp notification-interval 2178
lldp notifications 2179
lldp port-number-type 2180
lldp reinit 2181
lldp run 2182
lldp timer 2183
lldp tlv-select 2184
lldp transmit receive 2186
lldp tx-delay 2187
location civic-location configuration 2188
location civic-location identifier 2193
location civic-location-id 2194
location coord-location configuration 2195
location coord-location identifier 2197
location coord-location-id 2198
location elin-location 2199
location elin-location-id 2200
log buffered (filter) 309
log buffered 308
log buffered size 312
log console (filter) 314
log console 313
log email (filter) 318
log email 317
log email time 322
log host (filter) 325
log host 324
log host time 329
log monitor (filter) 331
log permanent (filter) 335
log permanent 334
log permanent size 338
login authentication size 338
logout 91
log-rate-limit nsm 339
loop-protection 393
loop-protection action 395
loop-protection action-delay-time 396
loop-protection timeout 397
mac address-table acquire 398
mac address-table ageing-time 399
mac address-table static 400
mac address-table trash-limit 401
mail 2227
mail from 2228
mail smtpserver 2229
match access-group 1430
match cos 1432
match dscp 1433
match eth-format protocol 1434
match inner-cos 1437
match inner-vlan 1438
match interface 1022
match ip address 1023
match ip next-hop 1025
match ip-precedence 1439
match ipv6 address 1027
match mac-type 1440
match metric 1028
match route-type 1029
match tag 1030
match tcp-flags 1441
match vlan 1442
max-concurrent-dd (IPv6 OSPF) 968
max-concurrent-dd 866
max-fib-routes 237
maximum-access-list 1372
maximum-area 867
maximum-paths 731
maximum-prefix 769
max-static-routes 238
mirror interface 402
mkdir 160
mls qos cos 1443
mls qos enable 1444
mls qos map cos-queue to 1445
mls qos map premark-dscp to 1446
move 161
move debug 162
mrq 359
mtu 361
multicast 1060
nas 1691
neighbor (IPv6 RIPng) 802
neighbor (OSPF) 868
neighbor (RIP) 770
network (DHCP) 2047
network (RIP) 771
network area 869
next-server 2048
no debug all 239
no police 1448
normal-interval 2293
ntp access-group 2003
ntp authenticate 2004
ntp authentication-key 2005
ntp broadcastdelay 2006
ntp master 2007
ntp peer 2008
ntp server 2010
ntp source 2012
ntp trusted-key 2014
offset-list (IPv6 RIPng) 803
offset-list (RIP) 772
optimistic-nd 669
option (DHCPv6) 2110
option 2049
ospf abr-type 870
ospf restart grace-period 871
ospf restart helper 872
ospf router-id 874
overflow database 875
overflow database external 876
passive-interface (IPv6 OSPF) 969
passive-interface (IPv6 RIPng) 804
passive-interface (OSPF) 877
passive-interface (RIP) 773
ping 670
ping ipv6 720
ping-poll 2294
platform hwfilter-size 404
platform I3-vlan-hashing-algorithm 1588
platform load-balancing 405
platform mac-vlan-hashing-algorithm 1589
platform stop-unreg-mc-flooding 406
platform vlan-stacking-tpid 408
polarity 409
police single-rate action 1449
police twin-rate action 1451
policy-map 1453
port-vlan-forwarding-priority 446
power-inline allow-legacy 598
power-inline description 599
power-inline enable 600
power-inline max 601
power-inline priority 603
power-inline usage-threshold 605
preempt-mode 1822
prefix-delegation pool 2112
priority 1824
priority-queue 1454
private-vlan 449
private-vlan association 450
privilege level 109
probe enable 2051
probe packets 2052
probe timeout 2053
probe type 2054
pwd 163
radius-server deadtime 1652
radius-server host 1653
radius-server key 1656
radius-server local 1692
radius-server retransmit 1657
radius-server timeout 1659
range 2055
reboot 240
reboot rolling 2335
recv-buffer-size (IPv6 RIPng) 805
recv-buffer-size (RIP) 774
redistribute (IPv6 OSPF) 970
redistribute (IPv6 RIPng) 806
redistribute (OSPF) 878
redistribute (RIP) 775
region (MSTP) 504
reload 241
reload rolling 2336
remark new-cos 1457
remark-map 1455
remote-command (deleted) 2337
remote-login 2338
repeat 2252
restart ipv6 ospf graceful 972
restart ospf graceful 880
restart rip graceful 776
revision (MSTP) 505
rip restart grace-period 777
rmdir 164
rmon alarm 2234
rmon collection history 2236
rmon collection stats 2237
rmon event 2238
route (IPv6 RIPng) 807
route (RIP) 778
route 2056
route-map 1031
router ipv6 ospf 973
router ipv6 rip 808
router ipv6 vrrp (interface) 1827
router ospf 881
router rip 779
router vrrp (interface) 1826
router-id (IPv6 OSPF) 974
router-id 882
sample-size 2295
script 2253
security-password forced-change 111
security-password history 110
security-password lifetime 112
security-password minimum-categories 113
security-password minimum-length 114
security-password reject-expired-pwd 115
security-password warning 116
send-lifetime 780
server (Server Group) 1661
server auth-port 1693
server enable 1694
service advanced-vty 117
service dhcp-relay 2057
service dhcp-server 2058
service dhcp-snooping 1788
service http 118
service password-encryption 119
service power-inline 606
service ssh 1730
service telnet 120
service terminal-length (deleted) 121
service test 375
service-policy input 1459
set ip next-hop (PBR) 1460
set ip next-hop (route map) 1033
set metric 1034
set metric-type 1036
set tag 1037
sflow agent (address) 2310
sflow collector (address) 2312
sflow collector max-datagram-size 2314
sflow enable 2315
sflow max-header-size 2316
sflow polling-interval 2318
sflow sampling-rate 2319
show aaa local user locked 1645
show access-list (IPv4 Hardware ACLs) 1330
show access-list (IPv4 Software ACLs) 1373
show arp 671
show arp security 1790
show arp security interface 1791
show arp security statistics 1793
show atmfl 1945
show atmfl area 1949
show atmfl area nodes 1954
show atmfl area nodes-detail 1956
show atmfl area summary 1952
show atmfl backup 1958
show atmfl backup area 1961
show atmfl detail 1963
show atmfl group 1965
show atmfl group members 1967
show atmfl links 1969
show atmfl links detail 1970
show atmfl links statistics 1977
show atmfl memory 1982
show atmfl nodes 1984
show atmfl provision nodes 1985
show atmfl tech 1987
show atmfl working-set 1990
show auth two-step supplicant brief 1590
show auth-mac 1591
show auth-mac diagnostics 1592
show auth-mac interface 1593
show auth-mac sessionstatistics 1595
show auth-mac statistics interface 1596
show auth-mac supplicant 1597
show auth-mac supplicant interface 1599
show auth-web 1600
show auth-web diagnostics 1602
show auth-web interface 1604
show auth-web sessionstatistics 1607
show auth-web statistics interface 1608
show auth-web supplicant 1609
show auth-web supplicant interface 1610
show auth-web-server 1611
show auth-web-server page 1613
show autoboot 165
show banner login 1732
show boot 166
show class-map 1461
show clock 242
show continuous-reboot-prevention 244
show counter dhcp-client 2059
show counter dhcp-relay 2060
show counter dhcp-server 2063
show counter ipv6 dhcp-client 2114
show counter ipv6 dhcp-server 2116
show counter log 341
show counter mail 2230
show counter ntp 2015
show counter ping-poll 2297
show counter snmp-server 2129
show counter stack 2339
show cpu 245
show cpu history 248
show crypto key hostkey 1733
show crypto key pubkey-chain knownhosts 1734
show crypto key pubkey-chain userkey 1735
show crypto key userkey 1736
show crypto pki certificates 1695
show crypto pki certificates local-radius-all-users 1697
show crypto pki certificates user 1699
show crypto pki trustpoints 1701
show debugging 251
show debugging aaa 1646
show debugging arp security 1795
show debugging atm 1991
show debugging atm 1992
show debugging dot1x 1496
show debugging ep sr 1861
show debugging gvrp 628
show debugging igmp 1110
show debugging ip dhcp snooping 1796
show debugging ip dns forwarding 673
show debugging ip packet 674
show debugging ipv6 ospf 975
show debugging ipv6 pim sparse-mode 1246
show debugging ipv6 rip 809
show debugging lacp 580
show debugging lldp 2201
show debugging loop prot 410
show debugging mld 1151
show debugging mstp 506
show debugging ospf 883
show debugging pim dense-mode 1286
show debugging pim sparse-mode 1190
show debugging platform packet 411
show debugging power-inline 607
show debugging radius 1663
show debugging rip 782
show debugging sflow 2320
show debugging snmp 2133
show debugging stack 2343
show debugging trigger 2255
show debugging vrrp 1828
show dhcp lease 2065
show diagnostic channel-group 581
show dos interface 1375
show dot1x 1497
show dot1x diagnostics 1500
show dot1x interface 1502
show dot1x sessionstatistics 1507
show dot1x statistics interface 1508
show dot1x supplicant 1509
show dot1x supplicant interface 1512
show ecofriendly 252
show epsr <epsr-instance> 1870
show epsr <epsr-instance> counters 1871
show epsr 1862
show epsr common segments 1867
show epsr config-check 1868
show epsr counters 1872
show epsr summary 1873
show etherchannel 583
show etherchannel detail 584
show etherchannel summary 585
show exception log 342
show file 168
show file systems 169
show flowcontrol interface 412
show gvrp configuration 629
show gvrp machine 630
show gvrp statistics 631
show gvrp timer 632
show history 92
show hosts 676
show interface 363
show interface access-group 1332
show interface brief 368
show interface err-disabled 413
show interface memory 254
show interface status 369
show interface switchport 414
show ip access-list 1378
show ip dhcp binding 2067
show ip dhcp pool 2069
show ip dhcp server statistics 2074
show ip dhcp server summary 2076
show ip dhcp snooping 1797
show ip dhcp snooping acl 1798
show ip dhcp snooping agent-option 1801
show ip dhcp snooping binding 1804
show ip dhcp snooping interface 1806
show ip dhcp snooping statistics 1808
show ip dhcp-relay 2073
show ip dns forwarding 677
show ip dns forwarding cache 678
show ip dns forwarding server 679
show ip domain-list 680
show ip domain-name 681
show ip igmp groups 1111
show ip igmp interface 1113
show ip igmp proxy 1117
show ip igmp snooping mrouter 1118
show ip igmp snooping routermode 1119
show ip igmp snooping statistics 1120
show ip interface 682
show ip mroute 1061
show ip mvif 1063
show ip name-server 683
show ip ospf 884
show ip ospf border-routers 887
show ip ospf database 888
show ip ospf database asbr-summary 890
show ip ospf database external 891
show ip ospf database network 893
show ip ospf database nssa-external 895
show ip ospf database opaque-area 897
show ip ospf database opaque-as 898
show ip ospf database opaque-link 899
show ip ospf database router 900
show ip ospf database summary 902
show ip ospf interface 905
show ip ospf neighbor 906
show ip ospf route 908
show ip ospf virtual-links 909
show ip pim dense-mode interface 1287
show ip pim dense-mode interface detail 1289
show ip pim dense-mode mroute 1290
show ip pim dense-mode neighbor 1291
show ip pim dense-mode neighbor detail 1292
show ip pim dense-mode nexthop 1293
show ip pim sparse-mode bsr-router 1191
show ip pim sparse-mode interface 1192
show ip pim sparse-mode interface detail 1194
show ip pim sparse-mode local-members 1195
show ip pim sparse-mode mroute 1197
show ip pim sparse-mode mroute detail 1199
show ip pim sparse-mode neighbor 1201
show ip pim sparse-mode nexthop 1202
show ip pim sparse-mode rp mapping 1204
show ip pim sparse-mode rp-hash 1203
show ip prefix-list 1379
show ip protocols ospf 910
show ip protocols rip 783
show ip rip 784
show ip rip database 785
show ip rip interface 786
show ip route 732
show ip route database 735
show ip route summary 737
show ip rpf 1064
show ip sockets 684
show ip source binding 1811
show ip traffic 687
show ipv6 access-list (IPv6 Hardware ACLs) 1399
show ipv6 access-list (IPv6 Software ACLs) 1421
show ipv6 dhcp 2118
show ipv6 dhcp binding 2119
show ipv6 dhcp interface 2122
show ipv6 dhcp pool 2124
show ipv6 forwarding 721
show ipv6 interface brief 722
show ipv6 mif 1067
show ipv6 mld groups 1152
show ipv6 mld interface 1153
show ipv6 mld snooping mrouter 1154
show ipv6 mld snooping statistics 1155
show ipv6 mroute 1065
show ipv6 neighbors 723
show ipv6 ospf 976
show ipv6 ospf database 978
show ipv6 ospf database external 980
show ipv6 ospf database grace 983
show ipv6 ospf database inter-prefix 986
show ipv6 ospf database inter-router 989
show ipv6 ospf database intra-prefix 992
show ipv6 ospf database link 995
show ipv6 ospf database network 998
show ipv6 ospf database router 1000
show ipv6 ospf interface 1005
show ipv6 ospf neighbor 1007
show ipv6 ospf route 1009
show ipv6 ospf virtual-links 1010
show ipv6 pim sparse-mode bsr-router 1247
show ipv6 pim sparse-mode interface 1248
show ipv6 pim sparse-mode interface detail 1250
show ipv6 pim sparse-mode local-members 1251
show ipv6 pim sparse-mode mroute 1253
show ipv6 pim sparse-mode mroute detail 1255
show ipv6 pim sparse-mode neighbor 1257
show ipv6 pim sparse-mode nexthop 1258
show ipv6 pim sparse-mode rp mapping 1260
show ipv6 pim sparse-mode rp nexthop 1261
show ipv6 pim sparse-mode rp-hash 1259
show ipv6 prefix-list 1422
show ipv6 protocols rip 810
show ipv6 rip 811
show ipv6 rip database 812
show ipv6 rip interface 813
show ipv6 route 724
show ipv6 route summary 726
show lacp sys-id 586
show lacp-counter 587
show license 207
show license brief 209
show license brief member 213
show license member 211
show lldp 2203
show lldp interface 2205
show lldp local-info 2207
show lldp neighbors 2212
show lldp neighbors detail 2214
show lldp statistics 2218
show lldp statistics interface 2220
show location 2222
show log 343
show log config 346
show log permanent 349
show loop-protection 415
show mac address-table 417
show mac address-table thrash-limit 419
show mail 2231
show memory 256
show memory allocations 258
show memory history 260
show memory pools 262
show memory shared 263
show mirror 420
show mirror interface 421
show mls qos 1462
show mls qos interface 1463
show mls qos interface policer-counters 1466
show mls qos interface queue-counters 1468
show mls qos interface storm-status 1469
show mls qos maps cos-queue 1470
show mls qos maps premark-dscp 1471
show ntp associations 2017
show ntp status 2019
show ping-poll 2299
show platform 422
show platform classifier statistics utilization brief 423
show platform port 425
show policy-map 1472
show port etherchannel 588
show port-security interface 429
show port-security intrusion 430
show port-vlan-forwarding-priority 451
show power-inline 608
show power-inline counters 611
show power-inline interface 613
show power-inline interface detail 615
show privilege 122
show process 264
show provisioning (stack) 2345
show proxy-autoconfig-file 1614
show radius 1664
show radius local-server group 1702
show radius local-server nas 1703
show radius local-server statistics 1704
show radius local-server user 1706
show radius statistics 1666
show reboot history 267
show rmon alarm 2239
show rmon event 2240
show rmon history 2242
show rmon statistics 2244
show route-map 1038
show router-id 269
show running-config 171
show running-config access-list 175
show running-config as-path access-list 176
show running-config atmf 1993
show running-config dhcp 177
show running-config full 178
show running-config interface 179
show running-config ip pim dense-mode 182
show running-config ip pim sparse-mode 183
show running-config ip route 184
show running-config ipv6 access-list 185
show running-config ipv6 mroute 186
show running-config ipv6 prefix-list 187
show running-config ipv6 route 188
show running-config key chain 189
show running-config lldp 190
show running-config log 350
show running-config power-inline 191
show running-config prefix-list 192
show running-config route-map 193
show running-config router 194
show running-config router ipv6 vrrp 1830
show running-config router vrrp 1829
show running-config router-id 195
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config security-password</td>
<td>196</td>
</tr>
<tr>
<td>show running-config sflow</td>
<td>2322</td>
</tr>
<tr>
<td>show running-config snmp</td>
<td>2134</td>
</tr>
<tr>
<td>show running-config ssh</td>
<td>1737</td>
</tr>
<tr>
<td>show running-config stack</td>
<td>2344</td>
</tr>
<tr>
<td>show running-config trigger</td>
<td>2256</td>
</tr>
<tr>
<td>show security-password configuration</td>
<td>123</td>
</tr>
<tr>
<td>show security-password user</td>
<td>124</td>
</tr>
<tr>
<td>show sflow</td>
<td>2323</td>
</tr>
<tr>
<td>show sflow interface</td>
<td>2325</td>
</tr>
<tr>
<td>show snmp-server</td>
<td>2135</td>
</tr>
<tr>
<td>show snmp-server community</td>
<td>2136</td>
</tr>
<tr>
<td>show snmp-server group</td>
<td>2137</td>
</tr>
<tr>
<td>show snmp-server user</td>
<td>2138</td>
</tr>
<tr>
<td>show snmp-server view</td>
<td>2139</td>
</tr>
<tr>
<td>show spanning-tree</td>
<td>507</td>
</tr>
<tr>
<td>show spanning-tree brief</td>
<td>510</td>
</tr>
<tr>
<td>show spanning-tree mst</td>
<td>511</td>
</tr>
<tr>
<td>show spanning-tree mst config</td>
<td>512</td>
</tr>
<tr>
<td>show spanning-tree mst detail</td>
<td>513</td>
</tr>
<tr>
<td>show spanning-tree mst detail interface</td>
<td>515</td>
</tr>
<tr>
<td>show spanning-tree mst detail interface</td>
<td>520</td>
</tr>
<tr>
<td>show spanning-tree mst instance</td>
<td>517</td>
</tr>
<tr>
<td>show spanning-tree mst instance interface</td>
<td>518</td>
</tr>
<tr>
<td>show spanning-tree mst interface</td>
<td>519</td>
</tr>
<tr>
<td>show spanning-tree statistics</td>
<td>522</td>
</tr>
<tr>
<td>show spanning-tree statistics instance</td>
<td>524</td>
</tr>
<tr>
<td>show spanning-tree statistics instance interface</td>
<td>526</td>
</tr>
<tr>
<td>show spanning-tree statistics interface</td>
<td>528</td>
</tr>
<tr>
<td>show spanning-tree vlan range-index</td>
<td>532</td>
</tr>
<tr>
<td>show ssh</td>
<td>1739</td>
</tr>
<tr>
<td>show ssh client</td>
<td>1741</td>
</tr>
<tr>
<td>show ssh server</td>
<td>1742</td>
</tr>
<tr>
<td>show ssh server allow-users</td>
<td>1744</td>
</tr>
<tr>
<td>show ssh server deny-users</td>
<td>1745</td>
</tr>
</tbody>
</table>
show stack 2346
show stack resiliencylink 2352
show startup-config 197
show static-channel-group 590
show storm-control 431
show system 270
show system environment 271
show system interrupts 272
show system mac 273
show system pci device 275
show system pci tree 276
show system pluggable 277
show system pluggable detail 280
show system pluggable diagnostics 285
show system serialnumber 288
show tacacs+ 1712
show tech-support 289
show telnet 125
show test cable-diagnostics tdr 2329
show trigger 2257
show users 126
show version 198
show vlan 452
show vlan classifier group 453
show vlan classifier group interface 454
show vlan classifier interface group 455
show vlan classifier rule 456
show vlan private-vlan 457
show vlan statistics 458
show vrrp (session) 1837
show vrrp 1831
show vrrp counters 1834
show vrrp ipv6 1833
shutdown 372
snmp trap link-status 2140
snmp trap link-status suppress 2142
snmp-server 2144
snmp-server community 2146
snmp-server contact 2147
snmp-server enable trap 2148
snmp-server engineID local 2151
snmp-server engineID local reset 2153
snmp-server group 2154
snmp-server host 2156
snmp-server location 2158
snmp-server source-interface 2159
snmp-server startup-trap-delay 2160
snmp-server user 2161
snmp-server view 2164
snntp-address 2126
source-ip 2303
spanning-tree autoedge (RSTP and MSTP) 533
spanning-tree bpdu 534
spanning-tree cisco-interoperability (MSTP) 536
spanning-tree edgeport (RSTP and MSTP) 537
spanning-tree enable 538
spanning-tree errdisable-timeout enable 540
spanning-tree errdisable-timeout interval 541
spanning-tree force-version 542
spanning-tree forward-time 543
spanning-tree guard root 544
spanning-tree hello-time 545
spanning-tree link-type 546
spanning-tree max-age 547
spanning-tree max-hops (MSTP) 548
spanning-tree mode 549
spanning-tree mst configuration 550
spanning-tree mst instance 551
spanning-tree mst instance path-cost 552
spanning-tree mst instance priority 554
spanning-tree mst instance restricted-role 555
spanning-tree mst instance restricted-tcn 556
spanning-tree path-cost 558
spanning-tree portfast (STP) 559
spanning-tree portfast bpdu-filter 561
spanning-tree portfast bpdu-guard 563
spanning-tree priority (bridge priority) 565
spanning-tree priority (port priority) 566
spanning-tree restricted-role 567
spanning-tree restricted-tcn 568
spanning-tree transmit-holdcount 569
speed (asyn) 291
speed 433
ssh 1746
ssh client 1748
ssh server 1750
ssh server allow-users 1752
ssh server authentication 1754
ssh server deny-users 1756
ssh server resolve-host 1758
ssh server scp 1759
ssh server sftp 1760
stack disabled-master-monitoring 2354
stack enable 2355
stack management subnet 2357
stack management vlan 2358
stack priority 2359
stack renumber 2360
stack renumber cascade 2361
stack resiliencylink 2363
stack software-auto-synchronize 2365
stack virtual-chassis-id 2366
stack virtual-mac 2367
static-channel-group 591
storm-action 1473
storm-control level 435
storm-downtime 1474
storm-protection 1475
storm-rate 1476
storm-window 1477
subnet-mask 2077
summary-address (IPv6 OSPF) 1011
summary-address 911
switch provision (stack) 2368
switchport access vlan 459
switchport atmf-arealink remote-area 1994
switchport atmf-crosslink 1995
switchport atmf-link 1997
switchport enable vlan 460
switchport mode access 461
switchport mode private-vlan 462
switchport mode private-vlan trunk promiscuous 463
switchport mode private-vlan trunk secondary 465
switchport mode trunk 467
switchport port-security 436
switchport port-security aging 437
switchport port-security maximum 438
switchport port-security violation 439
switchport private-vlan host-association 468
switchport private-vlan mapping 469
switchport resiliencylink 2369
switchport trunk allowed vlan 470
switchport trunk native vlan 473
switchport vlan-stacking (double tagging) 475
switchport voice dscp 476
switchport voice vlan 477
switchport voice vlan priority 480
system territory (deprecated) 293
tacacs-server host 1713
tacacs-server key 1715
tacacs-server timeout 1716
tcpdump 693
telnet 127
telnet server 128
terminal length 129
terminal monitor 294
terminal resize 130
test 2262
test cable-diagnostics tdr interface 2330
test interface 376
thrash-limiting 440
time (trigger) 2263
timeout (ping polling) 2304
timers (IPv6 RIPng) 814
timers (RIP) 787
timers spf (IPv6 OSPF) (deprecated) 1013
timers spf exp (IPv6 OSPF) 1014
timers spf exp 912
traceroute 694
traceroute ipv6 727
transition-mode 1839
trap 2265
trigger 2266
trigger activate 2267
trust dscp 1478
type atmf node 1998
type atmf node 2268
type cpu 2271
type interface 2272
type memory 2273
type periodic 2274
type ping-poll 2275
type reboot 2276
type stack disabled-master 2277
type stack link 2278
type stack master-fail 2279
undebug aaa 1647
undebug atmf 2001
undebug dot1x 1515
undebug epsr 1874
undebug igmp 1121
undebug ip packet interface 695
undebug ipv6 ospf events 1015
undebug ipv6 ospf ifsm 1016
undebug ipv6 ospf lsa 1017
undebug ipv6 ospf nsm 1018
undebug ipv6 ospf packet 1019
undebug ipv6 ospf route 1020
undebug ipv6 pim sparse-mode 1264
undebug ipv6 rip 815
undebug lacp 593
undebug loopprot 442
undebug mail 2232
undebug mstp 570
undebug ospf events 913
undebug ospf ifsm 914
undebug ospf lsa 915
undebug ospf nsm 916
undebug ospf nsm 917
undebug ospf packet 918
undebug ospf route 919
undebug ping-poll 2306
undebug platform packet 443
undebug radius 1667
undebug rip 789
undebug sflow 2326
undebug snmp 2165
undebug ssh client 1761
undebug ssh server 1762
undebug stack 2371
undebug trigger 2283
undebug vrrp 1841
undebug vrrp events 1842
undebug vrrp packet 1843
up-count 2305
user (RADIUS server) 1708
username 131
version 790
virtual-ip 1844
virtual-ipv6 1846
vlan (RADIUS server) 1710
vlan 481
vlan classifier activate 482
vlan classifier group 483
vlan classifier rule ipv4 484
vlan classifier rule proto 485
vlan database 488
vlan mode stack-local-vlan 2370
vlan mode stack-local-vlan 489
vlan statistics 491
vrrp vmac 1848
wait 354
write file 200
write memory 201
write terminal 202
wrr-queue disable queues 1479
wrr-queue egress-rate-limit queues 1480
wrr-queue weight queues 1481
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 83
• “disable (Privileged Exec mode)” on page 84
• “do” on page 85
• “enable (Privileged Exec mode)” on page 86
• “end” on page 88
• “exit” on page 89
• “help” on page 90
• “logout” on page 91
• “show history” on page 92
**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>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;command&gt;</code></td>
<td>Specify the command and its parameters.</td>
</tr>
</tbody>
</table>

**Mode**  Any configuration mode

**Example**

```
awplus# configure terminal
awplus(config)# do ping 192.0.2.23
```
enable (Privileged Exec mode)

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;privilege-level&gt;</td>
<td>Specify the privilege level for a CLI session in the range &lt;1–15&gt;, 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.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec

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

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

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

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

The following example shows the `enable` command enabling access the Privileged Exec mode for users with a privilege level of 7 or greater. Users with a privilege level of 7 or greater do not need to enter a password to access Privileged Exec mode. Users with a privilege level 6 or less need to enter a password to access...
Privilege Exec mode. Use the `enable password` command or the `enable secret` commands to set the password to enable access to Privileged Exec mode.

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

**Related Commands**
- disable (Privileged Exec mode)
- enable password
- enable secret
- exit
- service password-encryption
- username
end

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

**Syntax**  end

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

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

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

**Related Commands**
- disable (Privileged Exec mode)
- enable (Privileged Exec mode)
- exit
**exit**

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

**Syntax**  `exit`

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

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

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

**Related Commands**  
- `disable (Privileged Exec mode)`
- `enable (Privileged Exec mode)`
- `end`
help

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

**Syntax**  help

**Mode**  All command modes

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

```
awplus# help
```

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

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

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

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

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

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

**Syntax**  logout

**Mode**  User Exec and Privileged Exec

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

```
awplus# logout
```
show history

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

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show history

**Mode**  User Exec and Privileged Exec

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

```
awplus# show history
```

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

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

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

- “clear line console” on page 95
- “clear line vty” on page 96
- “enable password” on page 97
- “enable secret” on page 100
- “exec-timeout” on page 103
- “flowcontrol hardware (asyn/console)” on page 105
- “length (asyn)” on page 107
- “line” on page 108
- “privilege level” on page 110
- “security-password history” on page 111
- “security-password forced-change” on page 112
- “security-password lifetime” on page 113
- “security-password minimum-categories” on page 114
- “security-password minimum-length” on page 115
- “security-password reject-expired-pwd” on page 116
- “security-password warning” on page 117
- “service advanced-vty” on page 118
- “service http” on page 119
- “service password-encryption” on page 120
- “service telnet” on page 121
- “service terminal-length (deleted)” on page 122
- “show privilege” on page 123
- “show security-password configuration” on page 124
- “show security-password user” on page 125
- “show telnet” on page 126
- “show users” on page 127
- “telnet” on page 128
- “telnet server” on page 129
- “terminal length” on page 130
- “terminal resize” on page 131
- “username” on page 132
clear line console

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

**Syntax**  clear line console 0

**Mode**  Privileged Exec

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

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

**Related Commands**  
clear line vty
flowcontrol hardware (asyn/console)
line
show users
**clear line vty**

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

**Syntax**  
clear line vty <0-32>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-32&gt;</td>
<td>Line number</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec

**Example**  
To reset the first vty line, use the command:  
```plaintext
awplus# clear line vty 1
```

**Related Commands**  
- privilege level
- line
- show telnet
- show users
enable password

**Overview** To set a local password to control access to various privilege levels, use the `enable password` Global Configuration command. Use the `enable password` command to modify or create a password to be used, and use the `no enable password` command to remove the password.

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

**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**

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;plain&gt;</code></td>
<td>Specifies the unencrypted password.</td>
</tr>
<tr>
<td>8</td>
<td>Specifies a hidden password will follow.</td>
</tr>
<tr>
<td><code>&lt;hidden&gt;</code></td>
<td>Specifies the hidden encrypted password. Use an encrypted password for better security where a password crosses the network or is stored on a TFTP server.</td>
</tr>
<tr>
<td>level</td>
<td>Privilege level &lt;1-15&gt;. 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 <code>no</code> 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.</td>
</tr>
</tbody>
</table>

**Default** The privilege level for enable password is level 15 by default. Previously the default was level 1.

**Mode** Global Configuration

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

A user can now have an intermediate CLI security level set with this command for privilege level 7 to access all the show commands in Privileged Exec mode and all
the commands in User Exec mode, but not any configuration commands in Privileged Exec mode.

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

**Using plain passwords**

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

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

This results in the following show output:

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

**Using encrypted passwords**

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

**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.

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

This results in the following show output:
USER ACCESS COMMANDS

ENABLE PASSWORD

Using hidden passwords

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

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

This results in the following show output:

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

**Related Commands**

- `enable` (Privileged Exec mode)
- `enable secret`
- `service password-encryption`
- `privilege level`
- `show privilege`
- `username`
- `show running-config`
enable secret

**Overview**

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

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

**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**

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>plain</code></td>
<td>Specifies the unencrypted password.</td>
</tr>
<tr>
<td>8</td>
<td>Specifies a hidden password will follow.</td>
</tr>
<tr>
<td><code>hidden</code></td>
<td>Specifies the hidden encrypted password. Use an encrypted password for better security where a password crosses the network or is stored on a TFTP server.</td>
</tr>
<tr>
<td><code>level</code></td>
<td>Privilege level &lt;1-15&gt;. 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 <code>no</code> 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.</td>
</tr>
</tbody>
</table>

**Default**

The privilege level for enable secret is level 15 by default.

**Mode**

Global Configuration

**Usage**

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

A user can have an intermediate CLI security level set with this command for privilege level 7 to access all the show commands in Privileged Exec mode and all the commands in User Exec mode, but not any configuration commands in Privileged Exec mode.
Note that the `enable secret` command is an alias for the `enable password` command and one password per privilege level is allowed using these commands. Do not assign one password to a privilege level with `enable password` and another password to a privilege level with `enable secret`. Use `enable password` or `enable secret` commands. Do not use both on the same level.

**Using plain passwords**

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

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

This results in the following show output:

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

**Using encrypted passwords**

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

**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.

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

This results in the following show output:

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

Enable Secret

Using hidden passwords

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

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

This results in the following show output:

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

Related Commands

- `enable` (Privileged Exec mode)
- `enable secret`
- `service password-encryption`
- `privilege level`
- `show privilege`
- `username`
- `show running-config`
exec-timeout

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

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

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

Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;minutes&gt;</td>
<td>&lt;0-35791&gt; Required integer timeout value in minutes</td>
</tr>
<tr>
<td>&lt;seconds&gt;</td>
<td>&lt;0-2147483&gt; Optional integer timeout value in seconds</td>
</tr>
</tbody>
</table>

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

Mode
Line Configuration

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

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

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

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

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

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

Validation
show running-config
USER ACCESS COMMANDS

EXEC-TIMEOUT

Related Commands

line
service telnet
flowcontrol hardware (asyn/console)

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

**Syntax**
```
flowcontrol hardware
no flowcontrol hardware
```

**Mode**
Line Configuration

**Default**
Hardware flow control is disabled by default.

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

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

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

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

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

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

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

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

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

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

Related Commands

clear line console
show running-config
speed (asyn)
length (asyn)

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-512&gt;</td>
<td>Number of lines on screen. Specify 0 for no pausing.</td>
</tr>
</tbody>
</table>

**Mode**
Line Configuration

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

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

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

**Examples**
To set the terminal session length on the console to 10 rows, use the command:

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

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

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

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

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

**Related Commands**
terminal resize
terminal length
### line

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;first-line&gt;</td>
<td>&lt;0-32&gt; Specify the first line number.</td>
</tr>
<tr>
<td>&lt;last-line&gt;</td>
<td>&lt;0-32&gt; Specify the last line number.</td>
</tr>
<tr>
<td>console</td>
<td>The console terminal line(s) for local access.</td>
</tr>
<tr>
<td>vty</td>
<td>Virtual terminal for remote console access.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

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

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

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

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

**Examples**
To enter Line Configuration mode in order to configure all VTYs, use the commands:
```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)#
```
To enter Line Configuration mode to configure the console (asyn 0) port terminal line, use the commands:

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

**Related Commands**

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


**privilege level**

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

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

**Mode**
Line Configuration

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

**Examples**
To set the console connection to have the maximum privilege level, use the following commands:

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

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

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

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

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

**Related Commands**
- `enable password`
- `line`
- `show privilege`
- `username`
**security-password history**

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

The **no security-password history** command disables the security password history functionality.

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

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

**Mode**  Global Configuration

**Examples**  
To restrict reuse of the three most recent passwords, use the command:
```
awplus# configure terminal
awplus(config)# security-password history 3
```

To allow the reuse of recent passwords, use the command:
```
awplus# configure terminal
awplus(config)# no security-password history
```

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

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

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

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

The `no security-password forced-change` command disables the forced-change feature.

**Syntax**  
```
security-password forced-change
```

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

**Default**  The forced-change feature is disabled by default.

**Mode**  Global Configuration

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

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

**Validation Commands**

```
show running-config security-password
show security-password configuration
```

**Related Commands**

- `security-password history`
- `security-password lifetime`
- `security-password minimum-categories`
- `security-password minimum-length`
- `security-password reject-expired-pwd`
- `security-password warning`
security-password lifetime

**Overview**
This command enables password expiry by specifying a password lifetime in days. Note that when the password lifetime feature is disabled, it also disables the `security-password forced-change` command and the `security-password warning` command.

The **no security-password lifetime** command disables the password lifetime feature.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-1000&gt;</td>
<td>Password lifetime specified in days. A value of 0 will disable lifetime functionality and the password will never expire. This is equivalent to the <code>no security-password lifetime</code> command.</td>
</tr>
</tbody>
</table>

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

**Mode**
Global Configuration

**Example**
To configure the password lifetime to 10 days, use the command:
```
awplus# configure terminal
awplus(config)# security-password lifetime 10
```

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4&gt;</td>
<td>Number of categories the password must satisfy, in the range 1 to 4.</td>
</tr>
</tbody>
</table>

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

**Mode**  Global Configuration

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-23&gt;</td>
<td>Minimum password length in the range from 1 to 23.</td>
</tr>
</tbody>
</table>

**Default**
The default minimum password length is 1.

**Mode**
Global Configuration

**Example**
To configure the required minimum password length as 8, use the command:
```
awplus# configure terminal
awplus(config)# security-password minimum-length 8
```

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

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

**Overview**

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

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

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

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

The **no security-password reject-expired-pwd** command disables the reject-expired-pwd feature.

**Syntax**

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

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

**Mode**
Global Configuration

**Example**

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

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

**Validation Commands**

- show running-config security-password
- show security-password configuration

**Related Commands**

- security-password history
- security-password forced-change
- security-password lifetime
- security-password minimum-categories
- security-password minimum-length
- security-password warning
- show security-password user
**security-password warning**

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

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

The `no security-password warning` command disables this feature.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;0-1000&gt;</code></td>
<td>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 <code>no security-password warning</code> command. The warning period must be less than, or equal to, the password lifetime set with the <code>security-password lifetime</code> command.</td>
</tr>
</tbody>
</table>

**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:

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

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

**Related Commands**  
- `security-password history`
- `security-password forced-change`
- `security-password lifetime`
- `security-password minimum-categories`
- `security-password minimum-length`
- `security-password reject-expired-pwd`
service advanced-vty

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

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

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

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

**Mode**  
Global Configuration

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

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

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

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

**Overview**  This command enables the HTTP (Hypertext Transfer Protocol) service. The HTTP service is enabled by default and is required to support the AlliedWare Plus™ GUI Java applet on a Java enabled browser.

The **no service http** command disables the HTTP feature.

**Syntax**

```
service http
no service http
```

**Default**  The HTTP service is enabled by default.

**Mode**  Global Configuration

**Examples**  To disable the HTTP service, use the command:

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

To re-enable the HTTP service after it has been disabled, use the following commands:

```
awplus# configure terminal
awplus(config)# service http
```
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
service terminal-length (deleted)

**Overview**  This command has been deleted.
show privilege

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

**Syntax**  show privilege

**Mode**  User Exec and Privileged Exec

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

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

```
awplus# show privilege
```

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

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

**Related Commands**  privilege level
show security-password configuration

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

**Syntax**  `show security-password configuration`

**Mode**  Privileged Exec

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

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

**Output**  Figure 2-2: Example output from the `show security-password configuration` command

<table>
<thead>
<tr>
<th>Security Password Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum password length</td>
<td>8</td>
</tr>
<tr>
<td>Minimum password character categories to match</td>
<td>3</td>
</tr>
<tr>
<td>Number of previously used passwords to restrict</td>
<td>4</td>
</tr>
<tr>
<td>Password lifetime</td>
<td>30 day(s)</td>
</tr>
<tr>
<td>Warning period before password expires</td>
<td>3 day(s)</td>
</tr>
<tr>
<td>Reject expired password at login</td>
<td>Disabled</td>
</tr>
<tr>
<td>Force changing expired password at login</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show running-config security-password`
- `show security-password user`
show security-password user

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

**Syntax**  
show security-password user

**Mode**  
Privileged Exec

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

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

**Output**  
Figure 2-3: Example output from the **show security-password** user command

<table>
<thead>
<tr>
<th>UserName</th>
<th>Privilege</th>
<th>Last-PWD-Change</th>
<th>Remaining-lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>manager</td>
<td>15</td>
<td>4625 day(s) ago</td>
<td>No Expiry</td>
</tr>
<tr>
<td>bob15</td>
<td>15</td>
<td>0 day(s) ago</td>
<td>30 days</td>
</tr>
<tr>
<td>ted7</td>
<td>7</td>
<td>0 day(s) ago</td>
<td>No Expiry</td>
</tr>
<tr>
<td>mike1</td>
<td>1</td>
<td>0 day(s) ago</td>
<td>No Expiry</td>
</tr>
</tbody>
</table>

**Related Commands**

- show running-config security-password
- show security-password configuration
show telnet

**Overview**  This command shows the Telnet server settings.

**Syntax**  show telnet

**Mode**  User Exec and Privileged Exec

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

```
awplus# show telnet
```

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

```
<table>
<thead>
<tr>
<th>Telnet Server Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>----------------------------</td>
</tr>
<tr>
<td>Telnet server: Enabled</td>
</tr>
<tr>
<td>Protocol: IPv4, IPv6</td>
</tr>
<tr>
<td>Port: 23</td>
</tr>
</tbody>
</table>
```

**Related Commands**  
- clear line vty
- service telnet
- show users
- telnet server
show users

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

**Syntax** `show users`

**Mode** User Exec and Privileged Exec

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

```
awplus# show users
```

**Output** Figure 2-5: Example output from the `show users` command

<table>
<thead>
<tr>
<th>Line</th>
<th>User</th>
<th>Host(s)</th>
<th>Idle</th>
<th>Location</th>
<th>Priv</th>
<th>Idletime</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>con 0</td>
<td>manager</td>
<td>idle</td>
<td>00:00:00</td>
<td>ttyS0</td>
<td>15</td>
<td>10</td>
<td>N/A</td>
</tr>
<tr>
<td>vty 0</td>
<td>bob</td>
<td>idle</td>
<td>00:00:03</td>
<td>172.16.11.3</td>
<td>1</td>
<td>0</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 2-1: Parameters in the output of the `show users` command

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>The TCP port to listen on.</td>
</tr>
<tr>
<td>default</td>
<td>Use the default TCP port number 23.</td>
</tr>
</tbody>
</table>

**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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;length&gt;</code></td>
<td><code>&lt;0-512&gt;</code> Number of rows that the device will display on the currently-active terminal before pausing.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Examples**  The following example sets the number of lines to 15:

```
awplus# terminal length 15
```

The following example removes terminal length set previously:

```
awplus# terminal no length
```

**Related Commands**

- `terminal resize`
- `length (asyn)`
**terminal resize**

**Overview**  Use this command to automatically adjust the number of rows of output on the console, which the device will display before pausing, to the number of rows configured on the user's terminal.

**Syntax**  terminal resize

**Mode**  User Exec and Privileged Exec

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

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

```
awplus# terminal resize
```

**Related Commands**  length (asyn)  terminal length
username

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

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

**Syntax**

```
username <name> privilege <0-15> [password [8] <password>]
username <name> password [8] <password>
no username <name>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>The login name for the user. Do not use punctuation marks such as single quotes (' '), double quotes (&quot; &quot;), or colons (: ) with the user login name.</td>
</tr>
<tr>
<td>privilege</td>
<td>The user's privilege level. Use the privilege levels to set the access rights for each user.</td>
</tr>
<tr>
<td>&lt;0-15&gt;</td>
<td>A privilege level: either 0 (no access), 1-14 (limited access) or 15 (full access). A user with privilege level 1-14 can only access higher privilege levels if an enable password has been configured for the level the user tries to access and the user enters that password. A user at privilege level 1 can access the majority of show commands. A user at privilege level 7 can access the majority of show commands including platform show commands. Privilege Level 15 (to access the Privileged Exec command mode) is required to access configuration commands as well as show commands in Privileged Exec.</td>
</tr>
<tr>
<td>password</td>
<td>A password that the user must enter when logging in.</td>
</tr>
<tr>
<td>8</td>
<td>Specifies that you are entering a password as a string that has already been encrypted, instead of entering a plain-text password. The running-config displays the new password as an encrypted string even if password encryption is turned off. Note that the user enters the plain-text version of the password when logging in.</td>
</tr>
</tbody>
</table>
| <password> | The user's password. The password can be up to 23 characters in length and include characters from up to four categories. The password categories are:  
  - uppercase letters: A to Z  
  - lowercase letters: a to z  
  - digits: 0 to 9  
  - special symbols: all printable ASCII characters not included in the previous three categories. The question mark ? cannot be used as it is reserved for help functionality. |

**Mode**  Global Configuration

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

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

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

**Examples**

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

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

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

```plaintext
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
Introduction

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

Filename Syntax and Keyword Usage

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

<table>
<thead>
<tr>
<th>When you copy a file...</th>
<th>Use this syntax:</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copying in local Flash memory</td>
<td>flash:[/][&lt;directory&gt;/]&lt;filename&gt;</td>
<td>To specify a file in the configs directory in Flash: flash:configs/example.cfg</td>
</tr>
<tr>
<td>Copying to or from a USB storage device</td>
<td>usb:[/][&lt;directory&gt;/]&lt;filename&gt;</td>
<td>To specify a file in the top-level directory of the USB stick: usb:example.cfg</td>
</tr>
<tr>
<td>Copying with HTTP</td>
<td>http://[[&lt;username&gt;:&lt;password&gt;@] (&lt;hostname&gt;</td>
<td>&lt;host-ip&gt;)[/&lt;filepath&gt;]/]&lt;filename&gt;</td>
</tr>
<tr>
<td>Copying with TFTP</td>
<td>tftp://[&lt;location&gt;][/&lt;directory&gt;]&lt;filename&gt;</td>
<td>To specify a file in the top-level directory of the server: tftp://172.1.1.1/example.cfg</td>
</tr>
<tr>
<td>Copying with SCP</td>
<td>scp://&lt;username&gt;@&lt;location&gt;[/&lt;directory&gt;][/&lt;filename&gt;]</td>
<td>To specify a file in the configs directory on the server, logging on as user &quot;bob&quot;: e.g. scp://bob@10.10.0.12/configs/example.cfg</td>
</tr>
</tbody>
</table>
FILE MANAGEMENT COMMANDS

**Valid characters**

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

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

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

**Syntax for directory listings**

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

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

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

<table>
<thead>
<tr>
<th>When you copy a file...</th>
<th>Use this syntax:</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copying with SFTP</td>
<td><code>sftp://[[&lt;location&gt;]/&lt;directory&gt;]/&lt;filename&gt;</code></td>
<td>To specify a file in the top-level directory of the server: <code>sftp://10.0.0.5/example.cfg</code></td>
</tr>
<tr>
<td>Copying to or from stack member Flash</td>
<td><code>&lt;hostname&gt;-&lt;stack_ID&gt;/flash:[//]&lt;directory&gt;/&lt;stack_member_filename&gt;</code></td>
<td>To specify a file in the configs directory on member 2 of a stack named vcstack: <code>vcstack-2/flash/configs/example.cfg</code></td>
</tr>
</tbody>
</table>
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.

In a stacked environment you can only access `flash` and `nvs` using the stack member filepath (e.g. `dir awplus-2/flash:/`). To access a USB storage device on a backup stack member, use the `remote-login` command.
FILE MANAGEMENT COMMANDS

Command List
- “autoboot enable” on page 138
- “boot config-file” on page 139
- “boot config-file backup” on page 141
- “boot system” on page 142
- “boot system backup” on page 144
- “cd” on page 145
- “copy current-software” on page 146
- “copy debug” on page 147
- “copy running-config” on page 148
- “copy startup-config” on page 149
- “copy (filename)” on page 150
- “copy zmodem” on page 152
- “create autoboot” on page 153
- “delete” on page 154
- “delete debug” on page 155
- “dir” on page 156
- “edit” on page 158
- “edit (filename)” on page 159
- “erase startup-config” on page 161
- “mkdir” on page 162
- “move” on page 163
- “move debug” on page 164
- “pwd” on page 165
- “rmdir” on page 166
- “show autoboot” on page 167
- “show boot” on page 168
- “show file” on page 170
- “show file systems” on page 171
- “show running-config” on page 173
- “show running-config access-list” on page 177
- “show running-config as-path access-list” on page 178
- “show running-config dhcp” on page 179
- “show running-config full” on page 180
- “show running-config interface” on page 181
- “show running-config ip pim dense-mode” on page 184
FILE MANAGEMENT COMMANDS

- “show running-config ip pim sparse-mode” on page 185
- “show running-config ip route” on page 186
- “show running-config ipv6 access-list” on page 187
- “show running-config ipv6 mroute” on page 188
- “show running-config ipv6 prefix-list” on page 189
- “show running-config ipv6 route” on page 190
- “show running-config key chain” on page 191
- “show running-config lldp” on page 192
- “show running-config power-inline” on page 193
- “show running-config prefix-list” on page 194
- “show running-config route-map” on page 195
- “show running-config router” on page 196
- “show running-config router-id” on page 197
- “show running-config security-password” on page 198
- “show startup-config” on page 199
- “show version” on page 200
- “write file” on page 202
- “write memory” on page 203
- “write terminal” on page 204
**autoboot enable**

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

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

![Example autoboot.txt file](image)

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

**NOTE:**

This command is not supported in a stacked configuration.

**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:

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

To disable the Autoboot feature, use the command:

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

**Related Commands**

- `create autoboot`
- `show autoboot`
- `show boot`
**boot config-file**

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filepath-filename&gt;</code></td>
<td>Filepath and name of a configuration file. The specified configuration file must exist in the specified filesystem. Valid configuration files must have a <code>.cfg</code> extension.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

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

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

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

**Examples**
To run the configuration file `branch.cfg` stored on the device’s Flash filesystem the next time the device boots up, use the commands:

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

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

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

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

```
awplus# configure terminal
awplus(config)# boot config-file usb:/branch.cfg
```
To remove the configuration file `branch.cfg` stored on the switch’s USB storage device filesystem the next time the device boots up, use the commands:

```bash
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
```

**Mode**  Global Configuration

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

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

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

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

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

**Related Commands**

- `boot config-file`
- `boot system`
- `boot system backup`
- `show boot`

**Parameter**  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filepath-filename&gt;</code></td>
<td>Filepath and name of a backup configuration file. Backup configuration files must be in the Flash filesystem. Valid backup configuration files must have a <code>.cfg</code> extension.</td>
</tr>
<tr>
<td>backup</td>
<td>The specified file is a backup configuration file.</td>
</tr>
</tbody>
</table>
FILE MANAGEMENT COMMANDS

BOOT SYSTEM

boot system

**Overview**
Use this command to set the release file to load during the next boot cycle. Use the **no** variant of this command to remove the release file as the boot file.

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

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

**Mode**
Global Configuration

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

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

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

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

**Examples**
To run the release file `x510-5.4.5-0.1.rel` stored on the device’s Flash filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# boot system flash:/x510-5.4.5-0.1.rel
```

To remove the release file `x510-5.4.5-0.1.rel` stored on the device’s Flash filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# no boot system flash:/x510-5.4.5-0.1.rel
```
To run the release file `x510-5.4.5-0.1.rel` stored on the switch’s USB storage device filesystem the next time the device boots up, use the commands:

```bash
awplus# configure terminal
awplus(config)# boot system usb:/x510-5.4.5-0.1.rel
```

To remove the release file `x510-5.4.5-0.1.rel` stored on the switch’s USB storage device filesystem the next time the device boots up, use the commands:

```bash
awplus# configure terminal
awplus(config)# boot system usb:/x510-5.4.5-0.1.rel
```

In a VCStack configuration, if there is not enough space to synchronize the new release across the stack, the boot system command has an interactive mode that prompts you to delete old releases.

```bash
awplus# configure terminal
awplus(config)# boot system x510-5.4.5-0.1.rel
```

```
Insufficient flash available on stack member-2 (11370496) to synchronize file x510-5.4.5-0.1.rel (14821895).
List of release files on stack member-2
  x510-5.4.5-0.1.rel (14822400)
Select files to free up space,
Delete awplus-2/flash:/x510-5.4.5-0.1.rel
? (y/n)[n]:y
```

```bash
awplus(config)# y
```

```
Deleting selected files, please wait............................
Successful operation
VCS synchronizing file across the stack, please wait.............
File synchronization with stack member-2 successfully completed
[DONE]
```

### Related Commands
- `boot config-file`
- `boot config-file backup`
- `boot system backup`
- `show boot`
**boot system backup**

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

Use the **no** variant of this command to remove the backup release file as the backup boot file.

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

**Mode**  Global Configuration

**Examples**  
To specify the file `x510-5.4.5-0.1.rel` as the backup to the main release file, use the commands:
```
awplus# configure terminal
awplus(config)# boot system backup flash:/x510-5.4.5-0.1.rel
```

To remove the file `x510-5.4.5-0.1.rel` as the backup to the main release file, use the commands:
```
awplus# configure terminal
awplus(config)# no boot system backup flash:/x510-5.4.5-0.1.rel
```

**Related Commands**  
- boot config-file
- boot config-file backup
- boot system
- show boot

**Parameter**  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filepath-filename&gt;</code></td>
<td>Filepath and name of a backup release file. Backup release files must be in the Flash filesystem. Valid release files must have a <code>.rel</code> extension.</td>
</tr>
<tr>
<td>backup</td>
<td>The specified file is a backup release file.</td>
</tr>
</tbody>
</table>
Overview
This command changes the current working directory.

Syntax
`cd <directory-name>`

Mode
Privileged Exec

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

```
awplus# cd images
```

Related Commands
- `dir`
- `pwd`
- `show file systems`
copy current-software

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;destination-name&gt;</code></td>
<td>The filename and path where you would like the current running-release saved. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See <a href="#">Introduction</a> on page 133 for valid syntax.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

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

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

**Related Commands**  
boot system backup
show boot
**copy debug**

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

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

**Parameter**  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;destination-name&gt;</code></td>
<td>The filename and path where you would like the debug output saved. See Introduction on page 133 for valid syntax.</td>
</tr>
<tr>
<td><code>&lt;source-name&gt;</code></td>
<td>The filename and path where the debug output originates. See Introduction on page 133 for valid syntax.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec

**Example**  
To copy debug output to a USB storage device with a filename `my-debug`, use the following command:
```
awplus# copy debug usb:mydebug
```

**Output**  
Figure 3-2: CLI prompt after entering the copy debug command
```
Enter source file name []:
```

**Related Commands**  
delete debug
move debug
COPY RUNNING-CONFIG

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

Syntax
```
copy <source-name> running-config

copy running-config [<destination-name>]

copy running-config startup-config
```

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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;source-name&gt;</code></td>
<td>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 133 for valid syntax.</td>
</tr>
<tr>
<td><code>&lt;destination-name&gt;</code></td>
<td>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 133 for valid syntax.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

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

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

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

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

**Related Commands**  `copy running-config`
copy (filename)

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;source-name&gt;</code></td>
<td>The filename and path of the source file. See Introduction on page 133 for valid syntax.</td>
</tr>
<tr>
<td><code>&lt;destination-name&gt;</code></td>
<td>The filename and path for the destination file. See Introduction on page 133 for valid syntax.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

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

1) uppercase letters: A to Z
2) lowercase letters: a to z
3) digits: 0 to 9
4) special symbols: all printable ASCII characters not included in the previous three categories. Including the following characters:

- `-`
- `/`
- `.`
- `_`
- `@`
- `=`
- `*`
- `:`
- `~`
- `?`
Do not use spaces or parentheses within filenames. Use hyphens or underlines instead.

**Examples**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

To copy the file `test.txt` from the top level of Flash on stack member 2 to the current directory in the stack master, use the command:

```
awplus# copy awplus-2/flash:/test.txt test.txt
```

Note that you must specify either the NVS or Flash filesystem on the (backup) stack member (flash: in this example).

**Related Commands**

- `copy zmodem`
- `edit (filename)`
- `show file systems`
**copy zmodem**

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

**Syntax**

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

```
copy zmodem
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;source-name&gt;</code></td>
<td>The filename and path of the source file. See Introduction on page 133 for valid syntax.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

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

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

**Related Commands**

- `copy (filename)`
- `show file systems`
create autoboot

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

**Syntax**  
```
create autoboot [usb]
```

**Mode**  Privileged Exec

**Example**  To create an autoboot.txt file on external media, use the command:
```
awplus# create autoboot usb
```

**Related Commands**  
- autoboot enable
- show autoboot
- show boot
delete

**Overview**
This command deletes files or directories.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>force</td>
<td>Ignore nonexistent filenames and never prompt before deletion.</td>
</tr>
<tr>
<td>recursive</td>
<td>Remove the contents of directories recursively.</td>
</tr>
<tr>
<td>&lt;filename&gt;</td>
<td>The filename and path of the file to delete. See Introduction on page 133 for valid syntax.</td>
</tr>
</tbody>
</table>

**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>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;source-name&gt;</td>
<td>The filename and path where the debug output originates. See Introduction on page 133 for valid URL syntax.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec

**Example**  
To delete debug output, use the following command:

```
awplus# delete debug
```

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

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

**Related Commands**  
copy debug
move debug
**dir**

**Overview**  This command lists the files on a filesystem. If no directory or file is specified then this command lists the files in the current working directory.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>List all files.</td>
</tr>
<tr>
<td>recursive</td>
<td>List the contents of directories recursively.</td>
</tr>
<tr>
<td>sort</td>
<td>Sort directory listing.</td>
</tr>
<tr>
<td>reverse</td>
<td>Sort using reverse order.</td>
</tr>
<tr>
<td>name</td>
<td>Sort by name.</td>
</tr>
<tr>
<td>size</td>
<td>Sort by size.</td>
</tr>
<tr>
<td>time</td>
<td>Sort by modification time (default).</td>
</tr>
<tr>
<td>&lt;filename&gt;</td>
<td>The name of the directory or file. If no directory or file is specified, then this command lists the files in the current working directory.</td>
</tr>
<tr>
<td>debug</td>
<td>Debug root directory</td>
</tr>
<tr>
<td>flash</td>
<td>Flash memory root directory</td>
</tr>
<tr>
<td>nvs</td>
<td>NVS memory root directory</td>
</tr>
<tr>
<td>usb</td>
<td>USB storage device root directory</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Usage**  In a stacked environment you can use the CLI on a stack master to access filesystems that are located on another stack member. The syntax is `<hostname>-<stack_ID>/flash:][/[/<directory>/]<stack_member_filename>`. For example, to specify a file in the configs directory on member 2 of a stack, enter:

```
awplus-2/flash:/configs/example.cfg
```

**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
```

To list the files within the Flash filesystem for stack member 2, use the command:

```
awplus# dir awplus-2/flash:
```

Note that you must specify the filesystem on the stack member (flash in this example).

**Related Commands**

- `cd`
- `pwd`
**Overview**

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename&gt;</td>
<td>Name of a file in the local Flash filesystem.</td>
</tr>
</tbody>
</table>

**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>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filename&gt;</code></td>
<td>The filename and path of the remote file. See <strong>Introduction</strong> on page 133 for valid syntax.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

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

1)  uppercase letters: A to Z
2)  lowercase letters: a to z
3)  digits: 0 to 9
4)  special symbols: all printable ASCII characters not included in the previous three categories. Including the following characters:

- `-`
- `/`
- `.
- `_`
- `@`
- `=`
- `:
- `*`
- `:
- `~`
- `?`

Do not use spaces or parentheses within filenames. Use hyphens or underlines instead.
**Example**  To view the file `bob.key` stored in the security directory of a TFTP server, use the command:

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

**Related Commands**
- `copy (filename)`
- `edit`
- `show file`
**FILE MANAGEMENT COMMANDS**

**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
**Overview**  This command makes a new directory.

**Syntax**  `mkdir <name>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;name&gt;</code></td>
<td>The name and path of the directory that you are creating.</td>
</tr>
</tbody>
</table>

**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`
**Overview**

This command renames or moves a file.

**Syntax**

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

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;source-name&gt;</code></td>
<td>The filename and path of the source file. See Introduction on page 133 for valid syntax.</td>
</tr>
<tr>
<td><code>&lt;destination-name&gt;</code></td>
<td>The filename and path of the destination file. See Introduction on page 133 for valid syntax.</td>
</tr>
</tbody>
</table>

**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. Specify whether the destination is Flash or USB when saving the software to the local filesystem.

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

**Mode**
Privileged Exec

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

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

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

**Related Commands**
copy debug
delete debug
**pwd**

**Overview**  This command prints the current working directory.

**Syntax**  `pwd`

**Mode**  Privileged Exec

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

```
awplus# pwd
```

**Related Commands**  `cd`
**FILE MANAGEMENT COMMANDS**

**rmdir**

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

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

**Mode**  Privileged Exec

**Usage**  In a stacked environment you can use the CLI on a stack master to access filesystems that are located on another stack member. Refer to the Introduction.

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

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

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

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

To remove a directory called *test* from the top level of the Flash filesystem, in stack member 3, use the command:

```
awplus# rmdir awplus-3/flash:/test
```

Note that you must specify the filesystem, ("flash:" in this example).

**Related Commands**
- `cd`
- `dir`
- `mkdir`
- `pwd`
show autoboot

**Overview**  This command displays the Autoboot configuration and status.

**Syntax**  show autoboot

**Mode**  Privileged Exec

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

```
awplus# show autoboot
```

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

```plaintext
awplus#show autoboot
Autoboot configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoboot status</td>
<td>enabled</td>
</tr>
<tr>
<td>USB file autoboot.txt exists</td>
<td>yes</td>
</tr>
<tr>
<td>Restore information on USB</td>
<td></td>
</tr>
<tr>
<td>Autoboot enable in autoboot.txt</td>
<td>yes</td>
</tr>
<tr>
<td>Restore release file (file exists)</td>
<td>x510-5.4.5-0.1.rel</td>
</tr>
<tr>
<td>Restore configuration file</td>
<td>network_1.cfg (file exists)</td>
</tr>
</tbody>
</table>
```

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

```plaintext
awplus#show autoboot
Autoboot configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoboot status</td>
<td>enabled</td>
</tr>
<tr>
<td>External media source</td>
<td>USB not found.</td>
</tr>
</tbody>
</table>
```

**Related Commands**  autoboot enable
create autoboot
show boot
show boot

**Overview**  
This command displays the current boot configuration.

**Syntax**  
`show boot`

**Mode**  
Privileged Exec

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

```
awplus# show boot
```

**Output**  
Figure 3-7: Example output from the *show boot* command with the current boot config set on a USB storage device

```
awplus#show boot
Boot configuration
----------------------------------------
Current software : x510-5.4.5-0.1.rel
Current boot image : usb:/SBx81CFC960-5.4.4-1.2.rel
Backup boot image : flash:/SBx81CFC960-5.4.4-1.1.rel
Default boot config: flash:/default.cfg
Current boot config: usb:/my.cfg (file exists)
Backup boot config: flash:/backup.cfg (file not found)
Autoboot status : enabled
```

Figure 3-8: Example output from the *show boot* command

```
awplus#show boot
Boot configuration
----------------------------------------
Current software : x510-5.4.5-0.1.rel
Current boot image : flash:/SBx81CFC960-5.4.4-1.2.rel
Backup boot image : flash:/SBx81CFC960-5.4.4-1.1.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 of the *show boot* command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current software</td>
<td>The current software release that the device is using.</td>
</tr>
<tr>
<td>Current boot image</td>
<td>The boot image currently configured for use during the next boot cycle.</td>
</tr>
</tbody>
</table>
FILE MANAGEMENT COMMANDS

SHOW BOOT

Table 3-1: Parameters in the output of the `show boot` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup boot image</td>
<td>The boot image to use during the next boot cycle if the device cannot load the main image.</td>
</tr>
<tr>
<td>Default boot config</td>
<td>The default startup configuration file. The device loads this configuration script if no file is set as the startup-config file.</td>
</tr>
<tr>
<td>Current boot config</td>
<td>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.</td>
</tr>
<tr>
<td>Backup boot config</td>
<td>The configuration file to use during the next boot cycle if the main configuration file cannot be loaded.</td>
</tr>
<tr>
<td>Autoboot status</td>
<td>The status of the Autoboot feature; either enabled or disabled.</td>
</tr>
</tbody>
</table>

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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename&gt;</td>
<td>Name of a file on the local Flash filesystem, or name and directory path of a file.</td>
</tr>
</tbody>
</table>

**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`
**FILE MANAGEMENT COMMANDS**

**SHOW FILE SYSTEMS**

**show file systems**

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

If this command is entered on the stack master, it will list the filesystems for all the stack members. A stack member heading is displayed to distinguish the different lists shown for each stack member.

**Syntax**  
```
show file systems
```

**Mode**  
Privileged Exec

**Examples**  
To display the filesystems for either a standalone device, or a complete stack, use the command:

```
awplus# show file systems
```

**Output**  
Figure 3-9:  Example output from the `show file systems` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size (B)</td>
<td>The total memory available to this filesystem. The units are given after the value and are M for Megabytes or k for kilobytes.</td>
</tr>
<tr>
<td>Free (B)</td>
<td>The total memory free within this filesystem. The units are given after the value and are M for Megabytes or k for kilobytes.</td>
</tr>
<tr>
<td>Type</td>
<td>The memory type used for this filesystem; one of: flash, system, nvs, usbstick, tftp, scp, sftp, http.</td>
</tr>
</tbody>
</table>
### FILE MANAGEMENT COMMANDS

#### SHOW FILE SYSTEMS

**Related Commands**
- **edit**
- **edit (filename)**
- **show file**

---

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>The file setting options: rw (read write), ro (read only).</td>
</tr>
<tr>
<td>Prefixes</td>
<td>The prefixes used when entering commands to access the filesystems; one of: flash system nvs usb tftp scp sftp http.</td>
</tr>
<tr>
<td>S/V/D</td>
<td>The memory type: static, virtual, dynamic.</td>
</tr>
<tr>
<td>Lcl / Ntwk</td>
<td>Whether the memory is located locally or via a network connection.</td>
</tr>
<tr>
<td>Avail</td>
<td>Whether the memory is accessible: Y (yes), N (no), - (not applicable)</td>
</tr>
</tbody>
</table>
show running-config

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

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

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show running-config

**Mode**  Privileged Exec and Global Configuration

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

```
awplus# show running-config
```
**Output**  Figure 3-10: Example output from the *show running-config* command
awplus#show running-config
!
service password-encryption
!
hostname MyNode
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4DJwOJGPr7YqoExA0GVasdE0
!
no service ssh
!
autoboot enable
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
snmp-server contact Documentation Area
snmp-server location New Zealand
!
aaa authentication enable default local
aaa authentication login default local
!
ip domain-lookup
!
no service dhcp-server
!
no ip multicast-routing
!
spanning-tree mode rstp
!
no spanning-tree rstp enable
!
switch 1 provision x510-28
!
vlan database
  vlan 2-15 state enable
!
interface port1.0.1-1.0.6
  switchport
  switchport mode access
!
interface port1.0.25-1.0.26
  switchport
  switchport mode access
  switchport access vlan 14
!
interface vlan1
  ip address 192.168.1.1/24
  ipv6 enable
  ipv6 mld
!
interface vlan12
  ip address 192.168.3.1/24
!
ipv6 forwarding
!
line con 0
line vty 0 4
!
end
FILE MANAGEMENT COMMANDS
SHOW RUNNING-CONFIG

Related Commands

- copy running-config
- show running-config access-list
show running-config access-list

Overview
Use this command to show the running system status and configuration details for access-list.
For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Syntax
show running-config access-list

Mode
Privileged Exec and Global Configuration

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

awplus# show running-config access-list

Output
Figure 3-11: Example output from the show running-config access-list command

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

Related Commands
copy running-config
show running-config
show running-config as-path access-list

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

**Syntax**  show running-config as-path access-list

**Mode**  Privileged Exec and Global Configuration

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

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

**Output**  Figure 3-12: Example output from the show running-config as-path access-list command

```
! ip as-path access-list wer permit knsmk
!     
```

**Related Commands**  copy running-config

  show running-config
show running-config dhcp

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

**Syntax**  show running-config dhcp

**Mode**  Privileged Exec and Global Configuration

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

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

**Output**  Figure 3-13: Example output from the `show running-config dhcp` command

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

**Related Commands**  
copy running-config 
show running-config
show running-config full

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show running-config full
```

**Mode**
Privileged Exec and Global Configuration

**Example**
To display the complete status and configuration of the running system, use the command:
```
awplus# show running-config full
```

**Related Commands**
copy running-config
show running-config
show running-config interface

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

**Syntax**  
```
show running-config interface [<interface-list>] [dot1x|ip igmp|ip multicast|ip pim dense-mode|ip pim sparse-mode|ipv6 rip|lacp|mstp|ospf|rip|rstp|stp]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface-list&gt;</code></td>
<td>The interfaces or ports to display information about. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen, e.g. <code>vlan2-8</code>, <code>port1.0.1-1.0.4</code>, or <code>sai-2</code>, or <code>po1-2</code></td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above, e.g. <code>port1.0.1,port1.0.4-1.0.6</code>. Do not mix interface types in a list</td>
</tr>
<tr>
<td>dot1x</td>
<td>Displays running configuration for 802.1X port authentication for the specified interfaces.</td>
</tr>
<tr>
<td>lacp</td>
<td>Displays running configuration for LACP (Link Aggregation Control Protocol) for the specified interfaces.</td>
</tr>
<tr>
<td>ip igmp</td>
<td>Displays running configuration for IGMP (Internet Group Management Protocol) for the specified interfaces.</td>
</tr>
<tr>
<td>ip multicast</td>
<td>Displays running configuration for general multicast settings for the specified interfaces.</td>
</tr>
<tr>
<td>ip pim sparse-mode</td>
<td>Displays running configuration for PIM-SM (Protocol Independent Multicast - Sparse Mode) for the specified interfaces.</td>
</tr>
<tr>
<td>ip pim dense-mode</td>
<td>Displays running configuration for PIM-DM (Protocol Independent Multicasting - Dense Mode) for the specified interfaces.</td>
</tr>
<tr>
<td>mstp</td>
<td>Displays running configuration for MSTP (Multiple Spanning Tree Protocol) for the specified interfaces.</td>
</tr>
<tr>
<td>ospf</td>
<td>Displays running configuration for OSPF (Open Shortest Path First) for the specified interfaces.</td>
</tr>
<tr>
<td>rip</td>
<td>Displays running configuration for RIP (Routing Information Protocol) for the specified interfaces.</td>
</tr>
<tr>
<td>ipv6 rip</td>
<td>Displays running configuration for RIPng (RIP for IPv6) for the specified interfaces.</td>
</tr>
</tbody>
</table>
Mode

Privileged Exec and Global Configuration

Examples

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

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

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

awplus# show running-config interface vlan1

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

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

To display the current OSPF configuration of your device for ports 1 to 6, use the command:

awplus# show running-config interface port1.0.1-port1.0.6 ospf

Output

Figure 3-14: Example output from a show running-config interface port1.0.2 command

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

Figure 3-15: Example output from the `show running-config interface` command

```
awplus#show running-config interface
interface port1.0.1-1.0.6
  switchport
  switchport mode access
!
interface port1.0.25-1.0.26
  switchport
  switchport mode access
  switchport access vlan 14
!
interface port1.0.27-1.0.28
  switchport
  switchport mode access
  switchport access vlan 15
!
interface vlan1
  ip address 192.168.1.1/24
  ipv6 enable
  ipv6 mld
!
interface vlan12
  ip address 192.168.3.1/24
!
interface vlan13
  ip address 192.168.2.1/24
```

Related Commands

- `copy running-config`
- `show running-config`
**show running-config ip pim dense-mode**

**Overview**  Use this command to show the running system status and configuration details for PIM-DM.

**Syntax**  `show running-config ip pim dense-mode`

**Mode**  Privileged Exec and Global Configuration

**Example**  To display the running system status and configuration details for PIM-DM, use the command:

`awplus# show running-config ip pim dense-mode`

**Output**  Figure 3-16: Example output from the `show running-config ip pim dense-mode` command

```
!  ip pim spt-threshold
  ip pim accept-register list 1
!```

**Related Commands**

- `copy running-config`
- `show running-config`
show running-config ip pim sparse-mode

**Overview**  Use this command to show the running system status and configuration details for PIM-SM.

**Syntax**  show running-config ip pim sparse-mode

**Mode**  Privileged Exec and Global Configuration

**Example**  To display the running system status and configuration details for PIM-SM, use the command:

```
awplus# show running-config ip pim sparse-mode
```

**Output**  Figure 3-17: Example output from the `show running-config ip pim sparse-mode` command

```plaintext
! ip pim spt-threshold
ip pim accept-register list 1
! 
```

**Related Commands**  
copy running-config
show running-config
show running-config ip route

**Overview**  Use this command to show the running system static IPv4 route configuration. For information on filtering and saving command output, see “Controlling “show” Command Output” of the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show running-config ip route

**Mode**  Privileged Exec and Global Configuration

**Example**  To display the running system static IPv4 route configuration, use the command:

```
awplus# show running-config ip route
```

**Output**  Figure 3-18:  Example output from the *show running-config ip route* command

```
!  
ip route 3.3.3.3/32 vlan3
ip route 3.3.3.3/32 vlan2
!
```

**Related Commands**  
copy running-config  
show running-config
show running-config ipv6 access-list

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show running-config ipv6 access-list

**Mode**  
Privileged Exec and Global Configuration

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

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

**Output**  
Figure 3-19: Example output from the `show running-config ipv6 access-list` command

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

**Related Commands**  
copy running-config  
show running-config
show running-config ipv6 mroute

**Overview**  Use this command to show the running system IPv6 multicast route configuration.

**Syntax**  `show running-config ipv6 mroute`

**Mode**  Privileged Exec and Global Configuration

**Example**  To display the running system IPv6 multicast route configuration, use the command:

```
awplus# show running-config ipv6 mroute
```

**Output**  Figure 3-20: Example output from the `show running-config ipv6 mroute` command

```
!  ipv6 route 3e11::/64 lo
  ipv6 route 3e11::/64 vlan2
  ipv6 route fe80::/64 vlan3
!
```

**Related Commands**
- `copy running-config`
- `show running-config`
show running-config ipv6 prefix-list

**Overview**  Use this command to show the running system status and configuration details for IPv6 prefix lists.

**Syntax**  show running-config ipv6 prefix-list

**Mode**  Privileged Exec and Global Configuration

**Example**  To display show the running system status and configuration details for IPv6 prefix lists, use the command:

awplus# show running-config ipv6 prefix-list

**Output**  Figure 3-21: Example output from the `show running-config ipv6 prefix-list` command

```
! ipv6 prefix-list sde seq 5 permit any !
```

**Related Commands**  
copy running-config  
show running-config
show running-config ipv6 route

**Overview**
Use this command to show the running system static IPv6 route configuration.

For information on filtering and saving command output, see “Controlling “show” Command Output” of the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
`show running-config ipv6 route`

**Mode**
Privileged Exec and Global Configuration

**Example**
To display the running system static IPv6 route configuration, use the command:

```
awplus# show running-config ipv6 route
```

**Output**
Figure 3-22: Example output from the `show running-config ipv6 route` command

```
!
ipv6 route 3e11::/64 lo
ipv6 route 3e11::/64 vlan2
ipv6 route fe80::/64 vlan3
!
```

**Related Commands**
copy running-config

show running-config
show running-config key chain

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

**Syntax**
```
show running-config key chain
```

**Mode**
Privileged Exec and Global Configuration

**Example**
To display the running system key-chain related configuration, use the command:
```
awplus# show running-config key chain
```

**Output**
Figure 3-23: Example output from the `show running-config key chain` command

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

**Related Commands**
copy running-config
show running-config
show running-config lldp

**Overview**  
This command shows the current running configuration of LLDP.

**Syntax**  
show running-config lldp

**Mode**  
Privileged Exec and Global Configuration

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

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

**Output**  
Figure 3-24: Example output from the `show running-config lldp` command

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

**Related Commands**  
`show lldp`
`show lldp interface`
show running-config power-inline

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

**Syntax**

```
show running-config power-inline
```

**Mode** Privileged Exec and Global Configuration

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

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

**Output** Figure 3-25: Example output from the `show running-config power-inline` command

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

**Related Commands**

- `power-inline usage-threshold`
- `show power-inline`
show running-config prefix-list

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

**Syntax**  show running-config prefix-list

**Mode**  Privileged Exec and Global Configuration

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

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

**Output**  Figure 3-26:  Example output from the `show running-config prefix-list` command

```
! ip prefix-list abc seq 5 permit any
ip prefix-list as description annai
ip prefix-list wer seq 45 permit any
!
```

**Related Commands**  
copy running-config

show running-config
show running-config route-map

**Overview**
Use this command to show the running system status and configuration details for route-map.

For information on filtering and saving command output, see “Controlling “show” Command Output” of the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```bash
show running-config route-map
```

**Mode**
Privileged Exec and Global Configuration

**Example**
To display the running system status and configuration details for route-map, use the command:
```bash
awplus# show running-config route-map
```

**Output**
Figure 3-27: Example output from the `show running-config route-map` command

```
! route-map abc deny 2
  match community 2
! route-map abc permit 3
  match route-type external type-2
  set metric-type type-1
! 
```

**Related Commands**
copy running-config

show running-config
show running-config router

**Overview**  Use the show running-config router command to display the current running configuration for a given router.

**Syntax**  show running-config router <protocol>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;protocol&gt;</td>
<td>ospf</td>
</tr>
<tr>
<td>ospf</td>
<td>Open Shortest Path First (OSPF)</td>
</tr>
<tr>
<td>rip</td>
<td>Routing Information Protocol (RIP)</td>
</tr>
<tr>
<td>ipv6 rip</td>
<td>IPv6 RIP</td>
</tr>
<tr>
<td>vrrp</td>
<td>Virtual Redundancy Routing Protocol (VRRP)</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec and Global Configuration

**Example**  To display the current running configuration for a given router, use the command:

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

**Output**  Figure 3-28:  Example output from the show running-config router command

```
!
router ospf
 network 192.168.1.0/24 area 0.0.0.0
 network 192.168.3.0/24 area 0.0.0.0
!
```

**Related Commands**  copy running-config

show running-config
show running-config router-id

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

Syntax
show running-config router-id

Mode
Privileged Exec and Global Configuration

Example
To display the running system global router ID configuration, use the command:
```
awplus# show running-config router-id
```

Output
Figure 3-29: Example output from the `show running-config router-id` command
```
! router-id 3.3.3.3
!
```

Related Commands
- copy running-config
- show running-config
show running-config security-password

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

**Syntax**  show running-config security-password

**Mode**  Privileged Exec and Global Configuration

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

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

**Output**  Figure 3-30:  Example output from the `show running-config security-password` command

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

**Related Commands**  
- show security-password configuration
- show security-password user
**show startup-config**

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show startup-config

**Mode**  Privileged Exec

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

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

**Output**  Figure 3-31: Example output from the **show startup-config** command

```
awplus# show startup-config
!
service password-encryption
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
no service ssh
!
service telnet
!
service http
!
no clock timezone
.
.
line con 0
line vty 0 4
!
end
```

**Related Commands**  boot config-file backup  
copy running-config  
copy startup-config  
erase startup-config  
show boot
show version

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

**Syntax**  `show version`

**Mode**  User Exec and Privileged Exec

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

```
awplus# show version
```
Output  Figure 3-32: Example output from the **show version** command

```
awplus#show version
AlliedWare Plus (TM) 5.4.3 19/11/12 13:22:32
Build name : x510-5.4.5-0.1.rel
Build type : RELEASE
NET-SNMP SNMP agent software
   (c) 1996, 1998-2000 The Regents of the University of California.
   All rights reserved;
   (c) 2001-2003, Networks Associates Technology, Inc. All rights reserved.
   (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.
   (c) 2003, Sun Microsystems, Inc. All rights reserved.
   (c) 2003-2006, Sparta, Inc. All rights reserved.
   (c) 2004, Cisco, Inc and Information Network
   Center of Beijing University of Posts and Telecommunications.
   All rights reserved.
RSA Data Security, Inc. MD5 Message-Digest Algorithm
   (c) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.
OpenSSL Library
   Copyright (C) 1998-2011 The OpenSSL Project. All rights reserved.
Original SSLeay License
   Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com).
sFlow(R) Agent Software
   Copyright (c) 2002-2006 InMon Corp.
DHCP Library
   Copyright (c) 2004-2012 by Internet Systems Consortium, Inc. (*ISC*)
   Copyright (c) 1995-2003 by Internet Software Consortium.
DHCP Bind
   Copyright (c) 2005 - 2008, Holger Zuleger HZnet. All rights reserved.
Application Interface Specification Framework
   Copyright (c) 2002-2004 MontaVista Software, Inc;
   Copyright (c) 2005-2010 Red Hat, Inc.
Hardware Platform Interface Library
   Copyright (c) 2004 by Intel Corp.
   Copyright (C) IBM Corp. 2004-2008.
Corosync Cluster Engine
   Copyright (c) 2002-2004 MontaVista Software, Inc. All rights reserved.
Portions of this product are covered by the GNU GPL, source code may be
downloaded from: http://www.alliedtelesis.co.nz/support/gpl/awp.html
```

**Related Commands**

- `boot system backup`
- `show boot`
write file

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

**Syntax**  write [file]

**Mode**  Privileged Exec

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

```
awplus# write file
```

**Related Commands**  
- copy running-config
- write memory
- show running-config
write memory

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

**Syntax**  write [memory]

**Mode**  Privileged Exec

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

```
awplus# write memory
```

**Related Commands**  
- `copy running-config`
- `write file`
- `show running-config`
**write terminal**

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

**Syntax**  `write terminal`

**Mode**  Privileged Exec

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

```
awplus# write terminal
```

**Related Commands**  `show running-config`
Introduction

Overview  This chapter provides an alphabetical reference for each of the License commands.

Command List  •  “license” on page 204
               •  “license member (deleted)” on page 206
               •  “show license” on page 207
               •  “show license brief” on page 209
               •  “show license member” on page 211
               •  “show license brief member” on page 213
**Overview**  This command activates the licensed software feature set on a standalone switch, or a stack of switches.

Use the **no** variant of this command to deactivate the licensed software feature set on a standalone switch, or a stack of switches.

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, and the AlliedWare Plus™ How To notes for information on obtaining them. Purchase licenses from your authorized dealer or reseller.

Only install feature licenses during scheduled maintenance for any devices in a live environment. For example, if a feature license includes EPSR, EPSR is restarted with a temporary loss of EPSR network traffic.

**Syntax**

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;label&gt;</td>
<td>A name for the feature license. To determine names already in use, use the <code>show license</code> command. This can be the default name supplied for the feature, or a renamed feature name.</td>
</tr>
<tr>
<td>&lt;key&gt;</td>
<td>The encrypted license key to enable a set of software features.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Usage**  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 to be accepted with the issued keys.

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.

In a stacked configuration, the `license` command will add a license to all stack members and the `no license` command will remove a license from all stack members.

You can add a license to a specified stack member after first using the `remote-login` command from the stack master. Adding or deleting licenses on individual switches can cause different members of the stack to have different features.
enabled, which may cause the stack to fail to operate correctly. Unbalanced stack members will not form a stack. Stack members require the same feature licenses to be balanced.

If you add a feature license you will be prompted at the console that the feature needs to restart. For example, if the feature license contains a license for the EPSR protocol, then that protocol will restart. This action may result in the loss of network traffic. Only install licenses in scheduled maintenance periods for devices in a live environment.

Note that operating the following features requires an x510 Premium License (AT-FL-x510-01):

- RIP
- OSPF
- PIMv4-SM, DM, & SSM
- EPSR Master
- VLAN Double Tagging (Q in Q)
- RIPng
- OSPFv3
- MLDv1 & v2
- PIMv6-SM

**Examples**

To activate the license `name1` with the key `12345678ABCDE123456789ABCDE`, use the command:
```
awplus# license name1 12345678ABCDE123456789ABCDE
```

To deactivate the license `name1`, use the command:
```
awplus# no license name1
```

**Output**

Figure 4-1: Example of a license command entry to remove a feature license

```
awplus# no license IPv6
Stack member 1: Removal of "IPv6" will disable the following features:
    IPv6
INFO: Uninstalling license key will disable the affected modules immediately.
Would you like to continue? (y/n): y
Stack member 1 removed 1 license
1 license removed.
```

**Validation Command**

`show license`
Overview

This command has been deleted. Instead, use the `license` command to apply licenses to VCStack members.

In a stacked configuration, the `license` command will add a license to all stack members and the `no license` command will remove a license from all stack members.
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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>feature</td>
<td>Only display license information for any applied feature licenses.</td>
</tr>
<tr>
<td>&lt;label&gt;</td>
<td>The license name of the software feature to show information about. The license name can be used instead of the index number to identify a specific license.</td>
</tr>
<tr>
<td>index</td>
<td>The index number of the software feature license to show information about. The index number can be used instead of the license name to identify a specific license.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Usage**  This command will display licenses applied to a stack master only.

In a stacked configuration, use the `show license member` command instead if you need to display license information for a specific stack member or all stack members.

**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
```
LICENSING COMMANDS
SHOW LICENSE

**Output**  Figure 4-2: Example output from the `show license` command showing a base license with index 1

```sql
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            : 12-Jul-2014
License expiry date           : N/A
Features included             : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100, VCS, VRRP
------------------------------------------------------------------------
Index                         : 2
License name                  : 5.4.4
Customer name                 : 5.4.4
Quantity of licenses          : -
Type of license               : Trial
License issue date            : 12-Dec-2013
License expiry date           : N/A
Release                       : 5.4.4
```

Table 4-1: Parameters in the output of the `show license` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board region</td>
<td>Name of the region for the Base License features.</td>
</tr>
<tr>
<td>Index</td>
<td>Index identifying entry. The index is assigned automatically by the software. It is not configured.</td>
</tr>
<tr>
<td>License name</td>
<td>Name of the license key bundle (case-sensitive).</td>
</tr>
<tr>
<td>Customer name</td>
<td>Customer name.</td>
</tr>
<tr>
<td>Quantity of licenses</td>
<td>Quantity of licensed installations.</td>
</tr>
<tr>
<td>Type of license</td>
<td>Full or Trial.</td>
</tr>
<tr>
<td>License issue date</td>
<td>Date the license was generated.</td>
</tr>
<tr>
<td>License expiry date</td>
<td>Expiry date for trial license.</td>
</tr>
<tr>
<td>Features included</td>
<td>List of features included in the feature license.</td>
</tr>
</tbody>
</table>

**Related Commands**

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>feature</td>
<td>Only display license information for any applied feature licenses.</td>
</tr>
<tr>
<td>&lt;label&gt;</td>
<td>The license name of the software feature to show information about. The license name can be used instead of the index number to identify a specific license.</td>
</tr>
<tr>
<td>index</td>
<td>The index number of the software feature license to show information about. The index number can be used instead of the license name to identify a specific license.</td>
</tr>
<tr>
<td>&lt;index-number&gt;</td>
<td>Displays a brief summary of feature license information.</td>
</tr>
</tbody>
</table>

Mode  User Exec and Privileged Exec

Usage  This command will display licenses applied to a stack master only.

In a stacked configuration, use the show license brief member command instead if you need to display license information for a specific stack member or all stack members.

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

```
awplus# show license feature brief
```

Output  Figure 4-3: Example output from the show license brief command

```
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, RADIUS-100, VCS, VRRP
```
Table 4-2: Parameters in the output of the `show license brief` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board region</td>
<td>Name of the region for the Base License features.</td>
</tr>
<tr>
<td>Index</td>
<td>Index identifying entry. The index is assigned automatically by the software. It is not configured.</td>
</tr>
<tr>
<td>License name</td>
<td>Name of the license key bundle (case-sensitive).</td>
</tr>
<tr>
<td>Quantity</td>
<td>Quantity of licensed installations.</td>
</tr>
<tr>
<td>Customer name</td>
<td>Customer name.</td>
</tr>
<tr>
<td>Type</td>
<td>Full or Trial.</td>
</tr>
<tr>
<td>Period</td>
<td>Expiry date for trial license.</td>
</tr>
<tr>
<td>Current enabled features for displayed licenses</td>
<td>List of features included in the license.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `license`
- `show license`
- `show license member`
show license member

**Overview**
Use this command to display information about either a specific software license, or all software feature licenses enabled on either a specific stack member or all stack members.

**Syntax**
```
show license [<label>] member [<1-8>|all]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;label&gt;</td>
<td>The name of the license to show information about.</td>
</tr>
<tr>
<td>&lt;1-8&gt;</td>
<td>The ID of the stack member to show information about.</td>
</tr>
<tr>
<td>all</td>
<td>Display information about all stack members.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Usage**
Use the `show license member all` command to display full list output of all licenses per stack member.

**Examples**
To display full information about all enabled licenses on all stack members, use the command:
```
awplus# show license member all
```
To display full information about all enabled licenses on stack member 2, use the command:
```
awplus# show license member 2
```
To display full information about the license name1 on all stack members, use the command:
```
awplus# show license name1 member all
```
Output  Figure 4-4:  Example output from the `show license member` command

```plaintext
awplus#show license member all
Board region: Global
Software Feature Licenses
------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Index</th>
<th>License name</th>
<th>Customer name</th>
<th>Quantity of licenses</th>
<th>Type of license</th>
<th>License issue date</th>
<th>License expiry date</th>
<th>Features included</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Base License</td>
<td>Base License</td>
<td>1</td>
<td>Full</td>
<td>12-Jul-2014</td>
<td>N/A</td>
<td>IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100, VCS, VRRP</td>
</tr>
<tr>
<td>2</td>
<td>PIM Trial</td>
<td>PIM Trial</td>
<td>10</td>
<td>30 day trial</td>
<td>12-Jul-2014</td>
<td>12-Jul-2014</td>
<td>PIM PIM-100</td>
</tr>
</tbody>
</table>
```

Table 4-3: Parameters in the output of the `show license member` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board region</td>
<td>Name of the region for the Base License features.</td>
</tr>
<tr>
<td>Index</td>
<td>Index identifying entry. The index is assigned automatically by the software. It is not configured.</td>
</tr>
<tr>
<td>License name</td>
<td>Name of the license key bundle (case-sensitive).</td>
</tr>
<tr>
<td>Customer name</td>
<td>Customer name.</td>
</tr>
<tr>
<td>Quantity of licenses</td>
<td>Quantity of licensed installations.</td>
</tr>
<tr>
<td>Type of license</td>
<td>Full or Trial.</td>
</tr>
<tr>
<td>License issue date</td>
<td>Date the license was generated.</td>
</tr>
<tr>
<td>License expiry date</td>
<td>Expiry date for trial license.</td>
</tr>
<tr>
<td>Features included</td>
<td>List of features included in the license.</td>
</tr>
</tbody>
</table>

Related Commands

- `license`
- `show license`
- `show license brief member`
show license brief member

**Overview**
Use this command to display information about either a specific software license, or all software feature licenses enabled on either a specific stack member or all stack members.

**Syntax**
```
show license [<label>] brief member [<1-8>|all]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;label&gt;</code></td>
<td>The name of the license to show information about.</td>
</tr>
<tr>
<td><code>brief</code></td>
<td>Display a brief summary of license information.</td>
</tr>
<tr>
<td><code>&lt;1-8&gt;</code></td>
<td>The ID of the stack member to show information about.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Display information about all stack members.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Usage**
Use the `show license brief member all` command for brief table output of all licenses per stack member.

**Examples**
To display a brief summary of information about all enabled licenses on stack member 2, use the command:
```
awplus# show license brief member 2
```
To display a brief summary about all enabled licenses on all stack members, use the command:
```
awplus# show license brief member all
```
To display a brief summary about the license `name1` on all stack members, use the command:
```
awplus# show license name1 brief member all
```
**Output**  
Figure 4-5: Example output from the `show license brief member` command

```
awplus#show license brief member 1
Board region: Global
Software Release Licenses
------------------------------------------------------------------------
1  Base License  1            Base License
    Full            N/A
Current enabled features for displayed licenses:
IPv6Basic,
LAG-FULL, MLDSnoop, RADIUS-100, VCS, VRRP
```

Figure 4-6: Example output from the `show license brief member` command

**Table 4-4:** Parameters in the output of the `show license brief member` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board region</td>
<td>Name of the region for the Base License features.</td>
</tr>
<tr>
<td>Index</td>
<td>Index identifying entry. The index is assigned automatically by the software. It is not configured.</td>
</tr>
<tr>
<td>License name</td>
<td>Name of the license key bundle (case-sensitive).</td>
</tr>
<tr>
<td>Quantity</td>
<td>Quantity of licensed installations.</td>
</tr>
<tr>
<td>Customer name</td>
<td>Customer name.</td>
</tr>
<tr>
<td>Type</td>
<td>Full or Trial.</td>
</tr>
<tr>
<td>Period</td>
<td>Expiry date for trial license.</td>
</tr>
<tr>
<td>Current enabled features for displayed licenses</td>
<td>List of features included in the license.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `license`
- `show license`
- `show license member`
5
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 218
- “banner login (system)” on page 220
- “banner motd” on page 222
- “clock set” on page 224
- “clock summer-time date” on page 225
- “clock summer-time recurring” on page 227
- “clock timezone” on page 229
- “continuous-reboot-prevention” on page 230
- “ecofriendly led” on page 232
- “ecofriendly lpi” on page 233
- “findme” on page 235
- “hostname” on page 237
- “max-fib-routes” on page 239
- “max-static-routes” on page 240
- “no debug all” on page 241
- “reboot” on page 242
- “reload” on page 243
- “show clock” on page 244
- “show continuous-reboot-prevention” on page 246
- “show cpu” on page 247
- “show cpu history” on page 250
- “show debugging” on page 253
- “show ecofriendly” on page 254
- “show interface memory” on page 256
- “show memory” on page 258
- “show memory allocations” on page 260
- “show memory history” on page 262
- “show memory pools” on page 264
- “show memory shared” on page 265
- “show process” on page 266
- “show reboot history” on page 269
- “show router-id” on page 271
- “show system” on page 272
- “show system environment” on page 273
- “show system interrupts” on page 274
SYSTEM CONFIGURATION AND MONITORING COMMANDS

- “show system mac” on page 275
- “show system pci device” on page 277
- “show system pci tree” on page 278
- “show system pluggable” on page 279
- “show system pluggable detail” on page 282
- “show system pluggable diagnostics” on page 287
- “show system serialnumber” on page 290
- “show tech-support” on page 291
- “speed (asyn)” on page 293
- “system territory (deprecated)” on page 295
- “terminal monitor” on page 296
- “undebug all” on page 297
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**  
```plaintext
banner exec <banner-text>
banner exec default
no banner exec
```

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

```
AlliedWare Plus (TM) 5.4.5 03/31/14 00:44:25
```

**Mode**  Global Configuration

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

```
awplus#configure terminal
awplus(config)#banner exec enable to move to Priv Exec mode
awplus(config)#exit
awplus#exit
awplus login: manager
Password:
enable to move to Priv Exec mode
awplus>
```

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

```bash
awplus#configure terminal
awplus(config)#no banner exec
awplus(config)#exit
awplus#exit
awplus login: manager
Password:
AlliedWare
Plus (TM) 5.4.5 03/31/14
13:03:59
awplus>
```

**Related Commands**

- `banner login (system)`
- `banner motd`
**banner login (system)**

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

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

**Syntax**
```
banner login

no banner login
```

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

**Mode**
Global Configuration

**Examples**
To configure a login banner to be displayed when you login, enter the following commands:

```
awplus#configure terminal
awplus(config)#banner login
Type CNTL/D to finish.
authorised users only
awplus(config)#exit
awplus#exit
authorised users only
awplus login: manager
Password:
AlliedWare
Plus (TM) 5.4.5 03/31/14
13:03:59
awplus>
```

To remove the login banner, enter the following commands:
**Related Commands**

- `banner exec`  
- `banner motd`
**banner motd**

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

Use the **no** variant of this command to not display a text MOTD (Message-of-the-Day) banner on login.

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

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

**Mode**
Global Configuration

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

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

To remove the login banner, enter the following commands:

```
```
**BANNER MOTD**

**Related Commands**

- `banner exec`
- `banner login (system)`

```
awplus>enable
awplus#configure terminal
awplus(config)#no banner motd
awplus(config)#exit
awplus#exit
awplus login: manager
Password: 
AlliedWare Plus (TM) 5.4.5 03/31/14
13:03:59
awplus>
```
**clock set**

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

**Syntax**  

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="">hh:mm:ss</a></td>
<td>Local time in 24-hour format</td>
</tr>
<tr>
<td>&lt;day&gt;</td>
<td>Day of the current month &lt;1-31&gt;</td>
</tr>
<tr>
<td>&lt;month&gt;</td>
<td>The first three letters of the current month.</td>
</tr>
<tr>
<td>&lt;year&gt;</td>
<td>Current year &lt;2000-2035&gt;</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

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

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

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

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

**Related Commands**  clock timezone
clock summer-time date

**Overview**
This command defines the start and end of summertime for a specific year only, and specifies summertime’s offset value to Standard Time for that year.

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

By default, the device has no summertime definitions set.

**Syntax**
```
clock summer-time <timezone-name> date <start-day> <start-month> <start-year> <start-time> <end-day> <end-month> <end-year> <end-time> <1-180>
no clock summer-time
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;timezone-name&gt;</td>
<td>A description of the summertime zone, up to 6 characters long.</td>
</tr>
<tr>
<td>date</td>
<td>Specifies that this is a date-based summertime setting for just the specified year.</td>
</tr>
<tr>
<td>&lt;start-day&gt;</td>
<td>Day that the summertime starts, in the range 1-31.</td>
</tr>
<tr>
<td>&lt;start-month&gt;</td>
<td>First three letters of the name of the month that the summertime starts.</td>
</tr>
<tr>
<td>&lt;start-year&gt;</td>
<td>Year that summertime starts, in the range 2000-2035.</td>
</tr>
<tr>
<td>&lt;start-time&gt;</td>
<td>Time of the day that summertime starts, in the 24-hour time format HH:MM.</td>
</tr>
<tr>
<td>&lt;end-day&gt;</td>
<td>Day that summertime ends, in the range 1-31.</td>
</tr>
<tr>
<td>&lt;end-month&gt;</td>
<td>First three letters of the name of the month that the summertime ends.</td>
</tr>
<tr>
<td>&lt;end-year&gt;</td>
<td>Year that summertime ends, in the range 2000-2035.</td>
</tr>
<tr>
<td>&lt;end-time&gt;</td>
<td>Time of the day that summertime ends, in the 24-hour time format HH:MM.</td>
</tr>
<tr>
<td>&lt;1-180&gt;</td>
<td>The offset in minutes.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Examples**
To set a summertime definition for New Zealand using NZST (UTC+12:00) as the standard time, and NZDT (UTC+13:00) as summertime, with the summertime set to begin on the 1st October 2007 and end on the 18th of March 2008:

```
awplus(config)# clock summer-time NZDT date 1 oct 2:00 2007 18 mar 2:00 2008 60
```

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

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

- clock summer-time recurring
- clock timezone
**clock summer-time recurring**

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

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

By default, the device has no summertime definitions set.

**Syntax**

```
clock summer-time <timezone-name> recurring <start-week> <start-day> <start-month> <start-time> <end-week> <end-day> <end-month> <end-time> <1-180>
no clock summer-time
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;timezone-name&gt;</td>
<td>A description of the summertime zone, up to 6 characters long.</td>
</tr>
<tr>
<td>recurring</td>
<td>Specifies that this summertime setting applies every year from now on.</td>
</tr>
<tr>
<td>&lt;start-week&gt;</td>
<td>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 &lt;start-week&gt; and sun for &lt;start-day&gt;.</td>
</tr>
<tr>
<td>&lt;start-day&gt;</td>
<td>Day of the week when summertime starts. Valid values are mon, tue, wed, thu, fri, sat or sun.</td>
</tr>
<tr>
<td>&lt;start-month&gt;</td>
<td>First three letters of the name of the month that summertime starts.</td>
</tr>
<tr>
<td>&lt;start-time&gt;</td>
<td>Time of the day that summertime starts, in the 24-hour time format HH:MM.</td>
</tr>
<tr>
<td>&lt;end-week&gt;</td>
<td>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 &lt;end-week&gt; and sun for &lt;end-day&gt;.</td>
</tr>
<tr>
<td>&lt;end-day&gt;</td>
<td>Day of the week when summertime ends. Valid values are mon, tue, wed, thu, fri, sat or sun.</td>
</tr>
<tr>
<td>&lt;end-month&gt;</td>
<td>First three letters of the name of the month that summertime ends.</td>
</tr>
<tr>
<td>&lt;end-time&gt;</td>
<td>Time of the day that summertime ends, in the 24-hour time format HH:MM.</td>
</tr>
<tr>
<td>&lt;1-180&gt;</td>
<td>The offset in minutes.</td>
</tr>
</tbody>
</table>

**Mode**  Global Configuration
Examples

To set a summertime definition for New Zealand using NZST (UTC+12:00) as the standard time, and NZDT (UTC+13:00) as summertime, with summertime set to start on the 1st Sunday in October, and end on the 3rd Sunday in March, use the command:

```
awplus(config)# clock summer-time NZDT recurring 1 sun oct 2:00 3 sun mar 2:00 60
```

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

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

Related Commands

clock summer-time date

clock timezone
clock timezone

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

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

By default, the system time is set to UTC.

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

Mode
Global Configuration

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

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

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

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

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

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

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

Related Commands
- clock set
- clock summer-time date
- clock summer-time recurring

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

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

**Parameter** | **Description**
---|---
`enable` | Enable the continuous reboot prevention feature.

`period` | Set the period of time in which reboot events are counted.

`<0-604800>` | Period value in seconds. The default is 600.

`threshold` | Set the maximum number of reboot events allowed in the specified period.

`<1-10>` | Threshold value. The default is 1.

`action` | Set the action taken if the threshold is exceeded.

`linkdown` | Reboot procedure continues and all switch ports and stack ports stay link-down. The reboot event is logged. This is the default action.

`logonly` | Reboot procedure continues normally and the reboot event is logged.

`stopreboot` | Reboot procedure stops until the user enters the key "c" via the CLI. Normal reboot procedure then continues and the reboot event is logged.

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

**Mode**  Global Configuration

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

To enable continuous reboot prevention, use the commands:

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

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

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

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

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

To disable continuous reboot prevention, use the commands:

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

Related Commands

- `show continuous-reboot-prevention`
- `show reboot history`
- `show tech-support`
ecofriendly led

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

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

**Syntax**  
```
ecofriendly led
no ecofriendly led
```

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

**Mode**  Global Configuration

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

In a stack environment, enabling the eco-friendly LED feature on the stack master will apply the feature to every member of the stack.

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**

```plaintext
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**
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:

```plaintext
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:

```plaintext
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:

```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no ecofriendly lpi
```
To disable the eco-friendly 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)# 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>|member <stack-ID>]
[timeout <duration>]
no findme
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports to flash. The port list can be:</td>
</tr>
<tr>
<td></td>
<td>• a switch port, e.g. port1.0.4</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of ports separated by a hyphen, e.g.</td>
</tr>
<tr>
<td></td>
<td>port1.0.1-1.0.4</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of ports and port ranges, e.g.</td>
</tr>
<tr>
<td></td>
<td>port1.0.1,port1.0.5-1.0.6.</td>
</tr>
<tr>
<td>&lt;stack-ID&gt;</td>
<td>Stack member number, from 1 to 8.</td>
</tr>
<tr>
<td>&lt;duration&gt;</td>
<td>Specify the duration in seconds within the range of 5-3600 seconds.</td>
</tr>
</tbody>
</table>

*Default*  By default all port LEDs flash for 60 seconds.

*Mode*  Privileged Exec

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

You can specify a particular stack member with the optional member parameter. All available interfaces are flashed by default.

**NOTE:** The interface and member parameters are mutually exclusive.

*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

To activate the Find Me feature for the default duration on stack member 2, use the following command:

awplus# findme member 2

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

On a stack, after the stack master is elected, the master will have a host name: `awplus` by default, and this also becomes the name of the stack. Individual stack members (excluding the master) will have a host name that is the stack name hyphenated with a numeric suffix. For example, `awplus-1`, `awplus-2` and so on.

The hostname command can then be used to change the stack name and the stack master's host name. For example, for the hostname `Lab` the stack master's host name will be `Lab` and the other stack members will have host names `Lab-1`, `Lab-2` and so on.

In case of stack master fail-over, or stack split, the new stack will use the previous stack name as its host name and the stack name, unless it is changed by executing the hostname command on the new stack master.

Use the `no` variant of this command to revert the hostname setting to its default (`awplus`).

**Syntax**

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;hostname&gt;</code></td>
<td>Specifies the name given to a specific device. Also referred to as the Node Name in AMF output screens.</td>
</tr>
</tbody>
</table>

**Default**  `awplus`

**Mode**  Global Configuration

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

**NOTE:** Within an AMF network, any device without a hostname applied will automatically be assigned a name based on its MAC address.

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

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

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

This changes the prompt to:

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

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

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

This changes the prompt to:

```
awplus(config)#
```

*NOTE: When AMF is configured, running the no hostname command will apply a hostname that is based on the MAC address of the device node, for example, node_0016_76b1_7a5e.*

**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. The operation of these parameters is explained in the Parameter / Description table shown below.

*NOTE: To set 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-fib-routes</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;1-4294967294&gt;</td>
<td>The allowable configurable range for setting the maximum number of FIB-routes.</td>
</tr>
<tr>
<td>&lt;1-100&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>warning-only</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 that FIB routes are set and reset using `max-fib-routes`.

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

*NOTE: To set dynamic FIB routes, use the `max-fib-routes` command.*

**Syntax**
```plaintext
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:
```plaintext
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.

The debugging facility is disabled by default.

**Syntax**  no debug all [dot1x|ipv6|nsm|ospf|vrrp]

**Parameter**  | **Description**
---|---
**dot1x**  | Turns off all debugging for IEEE 802.1X port-based network access-control.
**ipv6**  | Turns off all debugging for IPv6 (Internet Protocol version 6).
**nsm**  | Turns off all debugging for the NSM (Network Services Module).
**ospf**  | Turns off all debugging for OSPF (Open Path Shortest First).
**vrrp**  | Turns off all debugging for VRRP (Virtual Router Redundancy Protocol).

**Mode**  Global Configuration and Privileged Exec

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

```
awplus# no debug all
```

To disable all 802.1X debugging, use the command:

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

To disable all IPv6 debugging, use the command:

```
awplus# no debug all ipv6
```

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 VRRP debugging, use the command:

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

**Related Commands**  undebug all
reboot

**Overview**  
This command halts the device and performs a cold restart (also known as reload). It displays a confirmation request before restarting.  
You can reboot a stand-alone device, a stack, or a specified stack member.

**Syntax**  
```
reboot <stack-ID>
reload <stack-ID>
reboot
reload
```

**Mode**  
Privileged Exec

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

When restarting the whole stack, you can either use this `reboot` command to reboot all stack members immediately, or to minimize downtime, reboot the stack members in a rolling sequence by using the `reboot rolling` command.

**Examples**  
To restart the device, use the command:

To restart the stand-alone device, use the command:
```
awplus# reboot
reboot system? (y/n): y
```

To restart all devices in the stack, use the command:
```
awplus# reboot
Are you sure you want to reboot the whole stack? (y/n): y
```

To restart stack member 2, use the command:
```
awplus# reboot stack-member 2
reboot stack-member 2 system? (y/n): y
```

If the specified stack member ID does not exist in the current stack, the command is rejected.

**Related Commands**
```
reboot rolling
reload rolling
```
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 5-1: Example output from the `show clock` command for a device using New Zealand time

```
Local Time: Mon,  6 Aug 2007 13:56:06 +1200
UTC Time:   Mon,  6 Aug 2007 01:56:06 +0000
Timezone: NZST
Timezone Offset: +12:00
Summer time zone: NZDT
Summer time starts: Last Sunday in September at 02:00:00
Summer time ends: First Sunday in April at 02:00:00
Summer time offset: 60 mins
Summer time recurring: Yes
```

Table 5-1: Parameters in the output of the `show clock` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Time</td>
<td>Current local time.</td>
</tr>
<tr>
<td>UTC Time</td>
<td>Current UTC time.</td>
</tr>
<tr>
<td>Timezone</td>
<td>The current configured timezone name.</td>
</tr>
<tr>
<td>Timezone Offset</td>
<td>Number of hours offset to UTC.</td>
</tr>
<tr>
<td>Summer time zone</td>
<td>The current configured summertime zone name.</td>
</tr>
<tr>
<td>Summer time starts</td>
<td>Date and time set as the start of summer time.</td>
</tr>
<tr>
<td>Summer time ends</td>
<td>Date and time set as the end of summer time.</td>
</tr>
<tr>
<td>Summer time offset</td>
<td>Number of minutes that summer time is offset from the system's timezone.</td>
</tr>
<tr>
<td>Summer time recurring</td>
<td>Whether the device will apply the summer time settings every year or only once.</td>
</tr>
</tbody>
</table>
SYSTEM CONFIGURATION AND MONITORING COMMANDS
SHOW CLOCK

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 5-2: Example output from the `show continuous-reboot-prevention` command

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

**Related Commands**
- `continuous-reboot-prevention`
- `show reboot history`
### show cpu

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
```plaintext
show cpu [<stack-ID>] [sort {thrds|pri|sleep|runtime}]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;stack-ID&gt;</td>
<td>Stack member number, from 1 to 8.</td>
</tr>
<tr>
<td>sort</td>
<td>Changes the sorting order using the following fields. If you do not specify a field, then the list is sorted by percentage CPU utilization.</td>
</tr>
<tr>
<td>thrds</td>
<td>Sort by the number of threads.</td>
</tr>
<tr>
<td>pri</td>
<td>Sort by the process priority.</td>
</tr>
<tr>
<td>sleep</td>
<td>Sort by the average time sleeping.</td>
</tr>
<tr>
<td>runtime</td>
<td>Sort by the runtime of the process.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Usage**  
Entering this command on the stack master will display the information for all the stack members. A stack member heading will distinguish the different information for every stack member device.

**Examples**  
To show the CPU utilization of current processes, sorting them by the number of threads the processes are using, use the command:

```plaintext
awplus# show cpu sort thrds
```

Note that in a stack environment, executing this command on the stack master will show CPU utilization for all stack members.

To show CPU utilization for a specific stack member (in this case stack member 2), use the following command:

```plaintext
awplus# show cpu 2
```
**Output** Figure 5-3: Example output from the `show cpu` command

Stack member 2:

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**

<table>
<thead>
<tr>
<th>pid</th>
<th>name</th>
<th>thrd</th>
<th>cpu%</th>
<th>pri</th>
<th>state</th>
<th>sleep%</th>
<th>runtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>1544</td>
<td>hostd</td>
<td>1</td>
<td>2.8</td>
<td>20</td>
<td>run</td>
<td>0</td>
<td>120</td>
</tr>
<tr>
<td>1166</td>
<td>exfx</td>
<td>17</td>
<td>1.8</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>3846</td>
</tr>
<tr>
<td>1198</td>
<td>stackd</td>
<td>1</td>
<td>0.9</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>459</td>
</tr>
<tr>
<td>1284</td>
<td>aisexec</td>
<td>44</td>
<td>0.9</td>
<td>-2</td>
<td>sleep</td>
<td>0</td>
<td>2606</td>
</tr>
<tr>
<td>1</td>
<td>init</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>120</td>
</tr>
<tr>
<td>9772</td>
<td>sh</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9773</td>
<td>corerotate</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>853</td>
<td>syslog-ng</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>356</td>
</tr>
<tr>
<td>859</td>
<td>klogd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>910</td>
<td>inetd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>920</td>
<td>portmap</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>931</td>
<td>crond</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1090</td>
<td>openhpid</td>
<td>11</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>233</td>
</tr>
<tr>
<td>1111</td>
<td>hpiologd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1240</td>
<td>hsl</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>79</td>
</tr>
<tr>
<td>1453</td>
<td>authd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>85</td>
</tr>
<tr>
<td>1497</td>
<td>cntrd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>1520</td>
<td>epard</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>56</td>
</tr>
<tr>
<td>1571</td>
<td>imi</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>275</td>
</tr>
<tr>
<td>1594</td>
<td>irdpd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>23</td>
</tr>
<tr>
<td>1617</td>
<td>lacpd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>87</td>
</tr>
<tr>
<td>1638</td>
<td>mstpd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>75</td>
</tr>
<tr>
<td>1662</td>
<td>nsm</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>163</td>
</tr>
<tr>
<td>1685</td>
<td>ospfd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>35</td>
</tr>
<tr>
<td>1708</td>
<td>pdmd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>23</td>
</tr>
<tr>
<td>1729</td>
<td>pimd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>1751</td>
<td>ripd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>33</td>
</tr>
<tr>
<td>1775</td>
<td>ripngd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>25</td>
</tr>
<tr>
<td>1797</td>
<td>rmond</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>64</td>
</tr>
<tr>
<td>1963</td>
<td>ntpd</td>
<td>1</td>
<td>0.0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
<td>15</td>
</tr>
</tbody>
</table>

... 

Table 5-2: Parameters in the output of the `show cpu` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack member</td>
<td>Stack member number.</td>
</tr>
<tr>
<td>CPU averages</td>
<td>Average CPU utilization for the periods stated.</td>
</tr>
<tr>
<td>System load averages</td>
<td>The average number of processes waiting for CPU time for the periods stated.</td>
</tr>
</tbody>
</table>
Table 5-2: Parameters in the output of the **show cpu** command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current CPU load</td>
<td>Current CPU utilization specified by load types.</td>
</tr>
<tr>
<td>pid</td>
<td>Identifier number of the process.</td>
</tr>
<tr>
<td>name</td>
<td>A shortened name for the process</td>
</tr>
<tr>
<td>threds</td>
<td>Number of threads in the process.</td>
</tr>
<tr>
<td>cpu%</td>
<td>Percentage of CPU utilization that this process is consuming.</td>
</tr>
<tr>
<td>pri</td>
<td>Process priority state.</td>
</tr>
<tr>
<td>state</td>
<td>Process state; one of “run”, “sleep”, “zombie”, and “dead”.</td>
</tr>
<tr>
<td>sleep%</td>
<td>Percentage of time that the process is in the sleep state.</td>
</tr>
<tr>
<td>runtime</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Related Commands**

- show memory
- show memory allocations
- show memory history
- show memory pools
- show process
show cpu history

**Overview**  This command prints a graph showing the historical CPU utilization.
For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show [<stack-ID>] cpu history

**Mode**  User Exec and Privileged Exec

**Usage**  This command’s output displays three graphs of the percentage CPU utilization:

- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

If this command is entered on the stack master, it will print graphs for all the stack members. A stack member heading will be displayed to distinguish the different graphs for every stack member.

**Examples**  To display a graph showing the historical CPU utilization of the device, use the command:

```
awplus# show cpu history
```

To display the CPU utilization history graph for stack member 2, use the command:

```
awplus# show 2 cpu history
```

where 2 is the node id of the stack member.
Figure 5-4: Example output from the `show cpu history` command

```
Stack member
2:

Per second CPU load history

<table>
<thead>
<tr>
<th>100</th>
<th>90</th>
<th>80</th>
<th>70</th>
<th>60</th>
<th>50</th>
<th>40</th>
<th>30</th>
<th>20</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Oldest</th>
<th>Newest</th>
</tr>
</thead>
</table>

CPU load% per second (last 60 seconds)
* = average CPU load%

Per minute CPU load history

<table>
<thead>
<tr>
<th>100</th>
<th>*+</th>
</tr>
</thead>
<tbody>
<tr>
<td>90</td>
<td>+</td>
</tr>
<tr>
<td>80</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>+</td>
</tr>
<tr>
<td>10</td>
<td>+</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Oldest</th>
<th>Newest</th>
</tr>
</thead>
</table>

CPU load% per minute (last 60 minutes)
* = average CPU load%, + = maximum

Per (30) minute CPU load history

<table>
<thead>
<tr>
<th>100</th>
<th>+</th>
</tr>
</thead>
<tbody>
<tr>
<td>90</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Oldest</th>
<th>Newest</th>
</tr>
</thead>
</table>

CPU load% per 30 minutes (last 60 values / 30 hours)
* = average, - = minimum, + = maximum

...
SYSTEM CONFIGURATION AND MONITORING COMMANDS
SHOW CPU HISTORY

Related Commands
show memory
show memory allocations
show memory pools
show process
show debugging

Overview
This command displays information for all debugging options.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Syntax
show debugging

Default
This command runs all the show debugging commands in alphabetical order.

Mode
User Exec and Privileged Exec

Usage
This command displays all debugging information, similar to the way the show tech-support command displays all show output for use by Allied Telesis authorized service personnel only.

Example
To display all debugging information, use the command:

awplus# show debugging

Output
Figure 5-5: Example output from the show debugging command

```
awplus#show debugging
AAA debugging status:
    Authentication debugging is off
    Accounting debugging is off
% DHCP Snooping service is disabled

802.1X debugging status:

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

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

```
show ecofriendly

**Overview**  This command displays the switch’s eco-friendly configuration status. The ecofriendly led 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 5-6: 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 5-3: Parameters in the output of the show ecofriendly command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>The eco-friendly LED feature is disabled and port LEDs show the current state of the ports. This is the default setting.</td>
</tr>
<tr>
<td>off</td>
<td>The eco-friendly LED feature is enabled and power to the port LEDs is disabled.</td>
</tr>
<tr>
<td>normal (configuration overridden by eco button)</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 5-3: Parameters in the output of the `show ecofriendly` command (cont.)

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

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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**

```
show interface memory
show interface <port-list> memory
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports to display information about. The port list can be:</td>
</tr>
<tr>
<td></td>
<td>• a switch port (e.g. port1.0.4) a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.4, or sa1-2, or po1-2</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
</tbody>
</table>

**Mode** User Exec and Privileged Exec

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

```
awplus# show interface memory
```

To display the shared memory used by port1.0.1 and port1.0.5 to port1.0.6, use the command:

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

**Output** Figure 5-7: Example output from the show interface<port-list>memory command

```
awplus#show interface port1.0.1, port1.0.5-1.0.6 memory
Vlan blocking state shared memory usage
---------------------------------------------------------------
Interface  shmid  Bytes Used  natcch  Status
port1.0.1  393228  512       1
port1.0.5  491535  512       1
port1.0.6  557073  512       1
```
Figure 5-8: Example output from the `show interface memory` command

```
awplus#show interface memory
Vlan blocking state shared memory usage
---------------------------------------------
<table>
<thead>
<tr>
<th>Interface</th>
<th>shmid</th>
<th>Bytes Used</th>
<th>nattch</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.1</td>
<td>393228</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.2</td>
<td>458766</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.3</td>
<td>360459</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.4</td>
<td>524304</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.5</td>
<td>491535</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.6</td>
<td>557073</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.7</td>
<td>327690</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.8</td>
<td>655380</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.9</td>
<td>622611</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.21</td>
<td>950301</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.22</td>
<td>1048608</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.23</td>
<td>1015839</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>port1.0.24</td>
<td>1081377</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>lo</td>
<td>425997</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>po1</td>
<td>1179684</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>po2</td>
<td>1212453</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>sa3</td>
<td>1245222</td>
<td>512</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
```

**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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  `show memory [<stack-ID>] [sort {size|peak|stk}]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;stack-ID&gt;</code></td>
<td>Stack member number, from 1 to 8.</td>
</tr>
<tr>
<td>sort</td>
<td>Changes the sorting order for the list of processes. If you do not specify this, then the list is sorted by percentage memory utilization.</td>
</tr>
<tr>
<td>size</td>
<td>Sort by the amount of memory the process is currently using.</td>
</tr>
<tr>
<td>peak</td>
<td>Sort by the amount of memory the process is currently using.</td>
</tr>
<tr>
<td>stk</td>
<td>Sort by the stack size of the process.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Usage**  If this command is entered on the stack master, it will display corresponding memory utilization information for all the stack members. A stack member heading will display the information for every stack member device.

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

```
awplus# show memory
```
Output Figure 5-9: Example output from the show memory command

```
awplus#show memory
Stack member 1:
RAM total: 514920 kB; free: 382716; buffers: 16368 kB
user processes
-------------
pid name     mem%  size  peak  data  stk
962 pss       6  33112 36260 27696  244
1  init       0   348  1092  288  84
797 syslog-ng 0   816  2152  752  84
803 klogd     0   184  1244  124  84
843 inetd     0   256  1256  136  84
```

Table 5-4: Parameters in the output of the show memory command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack member</td>
<td>Stack member number.</td>
</tr>
<tr>
<td>RAM total</td>
<td>Total amount of RAM memory free.</td>
</tr>
<tr>
<td>free</td>
<td>Available memory size.</td>
</tr>
<tr>
<td>buffers</td>
<td>Memory allocated kernel buffers.</td>
</tr>
<tr>
<td>pid</td>
<td>Identifier number for the process.</td>
</tr>
<tr>
<td>name</td>
<td>Short name used to describe the process.</td>
</tr>
<tr>
<td>mem%</td>
<td>Percentage of memory utilization the process is currently using.</td>
</tr>
<tr>
<td>size</td>
<td>Amount of memory currently used by the process.</td>
</tr>
<tr>
<td>peak</td>
<td>Greatest amount of memory ever used by the process.</td>
</tr>
<tr>
<td>data</td>
<td>Amount of memory used for data.</td>
</tr>
<tr>
<td>stk</td>
<td>The stack size.</td>
</tr>
</tbody>
</table>

Related Commands
- show memory allocations
- show memory history
- show memory pools
- show memory shared
show memory allocations

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show memory allocations [<process>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;process&gt;</td>
<td>Displays the memory allocation used by the specified process.</td>
</tr>
</tbody>
</table>

**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 5-10:  Example output from the show memory allocations command

```
awplus#show memory allocations
Memory allocations for imi
----------------------------
Current 15093760 (peak 15093760)
Statically allocated memory:
  - binary/exe          :    1675264
  - libraries           :    8916992
  - bss/global data     :    2985984
  - stack               :     139264

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

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

**Related Commands**

- show memory
- show memory history
- show memory pools
- show memory shared
- show tech-support
show memory history

**Overview**  
This command prints a graph showing the historical memory usage.
For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show memory history <stack-ID>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;stack-ID&gt;</td>
<td>Stack member number, from 1 to 8.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Usage**  
This command’s output displays three graphs of the percentage memory utilization:
- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.
If entered on the stack master, this command will display corresponding memory utilization information for all the stack members. A stack member heading will be displayed to distinguish the different lists for every stack member.

**Examples**  
To show a graph displaying the historical memory usage for either a single unstacked device, or a complete stack, use the command:

```
awplus# show memory history
```

To show a graph displaying the historical memory usage for specific stack member (stack member 2 in this example) within a stack, use the command:

```
awplus# show memory history 2
```
**Output**  
Figure 5-11: Example output from the `show memory history` command

```
STACK member 2:
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Syntax
show memory pools [<process>]

Mode
User Exec and Privileged Exec

Example
To show the memory pools used by processes, use the command:

awplus# show memory pools

Output
Figure 5-12: Example output from the show memory pools command

Related Commands
show memory allocations
show memory history
show tech-support
show memory shared

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show memory shared

**Mode**  User Exec and Privileged Exec

**Example**  To display information about the shared memory allocation used on the device, use the command:

```
awplus# show memory shared
```

**Output**  Figure 5-13:  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**  sort

show memory allocations

show memory history

show memory
show process

**Overview**  
This command lists a summary of the current running processes.  
For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show process [<stack-ID>] [sort {cpu|mem}]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;stack-ID&gt;</td>
<td>Stack member number, from 1 to 8.</td>
</tr>
<tr>
<td>sort</td>
<td>Changes the sorting order for the list of processes.</td>
</tr>
<tr>
<td>cpu</td>
<td>Sorts the list by the percentage of CPU utilization.</td>
</tr>
<tr>
<td>mem</td>
<td>Sorts the list by the percentage of memory utilization.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Usage**  
For a stacked configuration, if this command is entered on the stack master, it will display the information for all the stack members. A stack member heading will be displayed to distinguish the different information for every stack member.

**Example**  
To display a summary of the current running processes, use the command:  
```
awplus# show process
```  
To display a summary of the current running processes on stack member 2, use the command:  
```
awplus# show process 2
```
Output  Figure 5-14: Example output from the `show process` command

Stack
member 2:

CPU load for 1 minute: 0%; 5 minutes: 3%; 15 minutes: 0%
RAM total: 514920 kB; free: 382600 kB; buffers: 16368 kB

user processes
-----------------
<table>
<thead>
<tr>
<th>pid</th>
<th>name</th>
<th>thrds</th>
<th>cpu%</th>
<th>mem%</th>
<th>pri</th>
<th>state</th>
<th>sleep%</th>
</tr>
</thead>
<tbody>
<tr>
<td>962</td>
<td>pss</td>
<td>12</td>
<td>0</td>
<td>6</td>
<td>25</td>
<td>sleep</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>init</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>sleep</td>
<td>0</td>
</tr>
<tr>
<td>797</td>
<td>syslog-ng</td>
<td>1</td>
<td>0</td>
<td>16</td>
<td>16</td>
<td>sleep</td>
<td>88</td>
</tr>
</tbody>
</table>

kernel threads
--------------
<table>
<thead>
<tr>
<th>pid</th>
<th>name</th>
<th>cpu%</th>
<th>pri</th>
<th>state</th>
<th>sleep%</th>
</tr>
</thead>
<tbody>
<tr>
<td>71</td>
<td>aio/0</td>
<td>0</td>
<td>20</td>
<td>sleep</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>events/0</td>
<td>0</td>
<td>10</td>
<td>sleep</td>
<td>98</td>
</tr>
</tbody>
</table>

Table 5-5: Parameters in the output from the `show process` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack member</td>
<td>Stack member number.</td>
</tr>
<tr>
<td>CPU load</td>
<td>Average CPU load for the given period.</td>
</tr>
<tr>
<td>RAM total</td>
<td>Total memory size.</td>
</tr>
<tr>
<td>free</td>
<td>Available memory.</td>
</tr>
<tr>
<td>buffers</td>
<td>Memory allocated to kernel buffers.</td>
</tr>
<tr>
<td>pid</td>
<td>Identifier for the process.</td>
</tr>
<tr>
<td>name</td>
<td>Short name to describe the process.</td>
</tr>
<tr>
<td>thrds</td>
<td>Number of threads in the process.</td>
</tr>
<tr>
<td>cpu%</td>
<td>Percentage of CPU utilization that this process is consuming.</td>
</tr>
<tr>
<td>mem%</td>
<td>Percentage of memory utilization that this process is consuming.</td>
</tr>
<tr>
<td>pri</td>
<td>Process priority.</td>
</tr>
<tr>
<td>state</td>
<td>Process state; one of “run”, “sleep”, “stop”, “zombie”, or “dead”.</td>
</tr>
<tr>
<td>sleep%</td>
<td>Percentage of time the process is in the sleep state.</td>
</tr>
</tbody>
</table>
SYSTEM CONFIGURATION AND MONITORING COMMANDS
SHOW PROCESS

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 [<stack-ID>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;stack-ID&gt;</code></td>
<td>Stack member number, from 1 to 8.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**  To show the reboot history of stack member 2, use the command:

```
awplus# show reboot history 2
```

**Output**  Figure 5-15: Example output from the `show reboot history` command

```
awplus#show
reboot history 2
Stack member 2:
<date>    <time>    <type>      <description>
------------------------
2014-01-10 01:42:04  Expected    User Request
2014-01-10 01:35:31  Expected    User Request
2014-01-10 01:16:25  Unexpected Rebooting due to critical process (network/nsm) failure!
2014-01-09 20:46:40  Unexpected Rebooting due to VCS duplicate member-ID
2014-01-09 19:56:16  Expected    User Request
2010-01-09 20:36:06  Unexpected Rebooting due to VCS duplicate master (Continuous reboot prevention)
2014-01-09 19:51:20  Expected    User Request
```

Table 5-6: Parameters in the output from the `show reboot history` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unexpected</td>
<td>Reboot is counted by the continuous reboot prevention feature if the reboot event occurs in the time period specified for continuous reboot prevention.</td>
</tr>
<tr>
<td>Expected</td>
<td>Reboot is not counted by continuous reboot prevention feature.</td>
</tr>
</tbody>
</table>
SHOW REBOOT HISTORY

Related Commands
- show continuous-reboot-prevention
- show tech-support

Table 5-6: Parameters in the output from the **show reboot history** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous reboot</td>
<td>A continuous reboot prevention event has occurred. The action taken is configured with the <code>continuous-reboot-prevention</code> command. The next time period during which reboot events are counted begins from this event.</td>
</tr>
<tr>
<td>prevention</td>
<td></td>
</tr>
<tr>
<td>user request</td>
<td>User initiated reboot via the CLI.</td>
</tr>
</tbody>
</table>
**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 5-16: Example output from the `show router-id` command

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

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show system

**Mode**  
User Exec and Privileged Exec

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

awplus# show system

**Usage**  
For a stacked configuration, if this command is entered on the stack master, it will display the information for all the stack members. A stack member heading will be displayed to distinguish the different information for every stack member.

**Output**  
Figure 5-17: Example output from the **show system** command

```
awplus# show system
Switch System Status Mon Mar 10 08:42:16 2014
Board ID Bay Board Name Rev Serial number
-------------------------------
Base 369 x510-28GTX A-0 A24SCA01M

RAM: Total: 495792 kB Free: 384904 kB
Flash:  63.0MB Used:  50.9MB Available:  12.1MB

Environment Status : Normal
Uptime : 0 days 16:31:49
Bootloader version : 2.0.12

Current software : x510-5.4.5-0.1.rel
Software version : 5.4.4
Build date : Mon Mar 03 13:42:20 NZST 2014

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

System Name
awplus
System Contact
System Location
```
show system environment

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax** show system environment

**Mode** User Exec and Privileged Exec

**Usage** For a stacked configuration, if this command is entered on the stack master, it will display the information for all the stack members. A stack member heading will be displayed to distinguish the different information for every stack member.

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

```
awplus# show system environment
```

**Output** Figure 5-18: Example output from the show system environment command

```
Stack Environment Monitoring Status

Stack member 1:
Overall Status: Normal

Resource ID: 1 Name: x510-28GTX

<table>
<thead>
<tr>
<th>ID</th>
<th>Sensor (Units)</th>
<th>Reading</th>
<th>Low Limit</th>
<th>High Limit</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fan: Fan 1 (Rpm)</td>
<td>4344</td>
<td>3000</td>
<td>-</td>
<td>Ok</td>
</tr>
<tr>
<td>2</td>
<td>Voltage: 1.8V (Volts)</td>
<td>1.804</td>
<td>1.617</td>
<td>1.978</td>
<td>Ok</td>
</tr>
<tr>
<td>3</td>
<td>Voltage: 1.0V (Volts)</td>
<td>0.995</td>
<td>0.896</td>
<td>1.099</td>
<td>Ok</td>
</tr>
<tr>
<td>4</td>
<td>Voltage: 3.3V (Volts)</td>
<td>3.291</td>
<td>2.960</td>
<td>3.613</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>Voltage: 5.0V (Volts)</td>
<td>5.066</td>
<td>4.477</td>
<td>5.498</td>
<td>Ok</td>
</tr>
<tr>
<td>6</td>
<td>Voltage: 1.2V (Volts)</td>
<td>1.187</td>
<td>1.072</td>
<td>1.318</td>
<td>Ok</td>
</tr>
<tr>
<td>7</td>
<td>Temp: CPU (Degrees C)</td>
<td>50</td>
<td>-10</td>
<td>90</td>
<td>Ok</td>
</tr>
</tbody>
</table>
```

**Related Commands** show system
show system interrupts

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show system interrupts

**Mode**  User Exec and Privileged Exec

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

```
awplus# show system interrupts
```

**Output**  Figure 5-19: 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
 120:    0  OpenPIC  Edge Enabled  0  Plugin XEM
BAD:
    0
```

**Related Commands**  show system environment
show system mac

**Overview**  
This command displays the physical MAC address available on a standalone switch, or a stack. This command also shows the virtual MAC address for a stack if the stack virtual MAC address feature is enabled with the `stack virtual-mac` or the `stack enable` command.

**Syntax**  
`show system mac`

**Mode**  
User Exec and Privileged Exec

**Usage**  
This command also displays the virtual MAC address, if the VCStack virtual MAC address feature is enabled with the `stack virtual-mac` command.

For more information, see the VCStack Feature Overview and Configuration Guide.

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

```
awplus# show system mac
```

**Output**  
Figure 5-20: Example output from the `show system mac` command

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

Figure 5-21: Example output showing how to use the stack virtual-mac command and the show system mac command

```
awplus#configure terminal
awplus(config)#stack virtual-mac
% Please check that the new MAC 0000.cd37.0065 is unique within the network.
% Save the config and restart the system for this change to take effect.
Member1#copy run start
Building configuration... [OK]
Member1#reload
reboot system? (y/n): y
... Rebooting at user request ...
Loading default configuration ....
awplus login: manager
Password:
awplus>show system mac
eccd.6d9d.4eed
Virtual MAC Address 0000.cd37.0065
```

**Related Commands**

stack virtual-mac
**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 5-22: Example output from the `show system pci device` command

```
awplus# show system pci device
00:0c.0 Class 0200: 11ab:00d1 (rev 01)
  Flags: bus master, 66Mhz, medium devsel, latency 128, IRQ 113
  Memory at 5ffff000 (32-bit, non-prefetchable) [size=4K]
  Memory at 58000000 (32-bit, non-prefetchable) [size=64M]

00:0d.0 Class 0200: 11ab:00d1 (rev 01)
  Flags: bus master, 66Mhz, medium devsel, latency 128, IRQ 116
  Memory at 57fff000 (32-bit, non-prefetchable) [size=4K]
  Memory at 50000000 (32-bit, non-prefetchable) [size=64M]
```

**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 5-23:  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 pluggable

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
```plaintext
show system pluggable [porto-list]
```

**Mode**  User Exec and Privileged Exec

**Usage**  Entering this command will display the information for all pluggable transceivers in the system. In a stack, a separate heading will be displayed to distinguish each stack member’s information.

**Example**  To display brief information about pluggable transceivers installed in port1.0.1 through port1.0.4, use the command:

```plaintext
awplus# show system pluggable port1.0.1-1.0.4
```

**Output**  
Figure 5-24: Example output from the `show system pluggable port1.0.1-1.0.4` command

<table>
<thead>
<tr>
<th>Port</th>
<th>Manufacturer</th>
<th>Device</th>
<th>Serial Number</th>
<th>Datecode</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.1</td>
<td>AGILENT</td>
<td>HFBR-5710L</td>
<td>0401312315461272</td>
<td>040131</td>
<td>1000BASE-SX</td>
</tr>
<tr>
<td>1.0.2</td>
<td>AGILENT</td>
<td>QBCU-5730R</td>
<td>AK0614GKF7</td>
<td>060408</td>
<td>1000BASE-T</td>
</tr>
<tr>
<td>1.0.3</td>
<td>AGILENT</td>
<td>HFBR-5710L</td>
<td>0305130112182696</td>
<td>030513</td>
<td>1000BASE-SX</td>
</tr>
<tr>
<td>1.0.4</td>
<td>AGILENT</td>
<td>HBCU-5710R</td>
<td>AK051300SM</td>
<td>050402</td>
<td>1000BASE-T</td>
</tr>
</tbody>
</table>

**Example**  To display information about the pluggable transceiver installed in port1.0.1, use the command:

```plaintext
awplus# show system pluggable port1.0.1
```
Output Figure 5-25: Example output from the `show system pluggable port1.0.1` command

<table>
<thead>
<tr>
<th>Port</th>
<th>Manufacturer</th>
<th>Device</th>
<th>Serial Number</th>
<th>Datecode</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.1</td>
<td>AGILENT</td>
<td>HFBR-5710L</td>
<td>0401312315461272</td>
<td>040131</td>
<td>1000BASE-SX</td>
</tr>
</tbody>
</table>

Figure 5-26: Example output from the `show system pluggable` command

Table 5-7: Parameters in the output from the `show system pluggables` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack member</td>
<td>The stack member number.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the vendor's name for the installed pluggable transceiver.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Specifies the vendor's name for the installed pluggable transceiver.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Specifies the device name for the installed pluggable transceiver.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Specifies the device type for the installed pluggable transceiver.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Specifies the serial number for the installed pluggable transceiver.</td>
</tr>
<tr>
<td>Manufacturing Datecode</td>
<td>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 &quot;How To Troubleshoot Fiber and Pluggable Issues&quot; in the &quot;Getting Started with AlliedWare Plus&quot; Feature Overview and Configuration Guide.</td>
</tr>
<tr>
<td>SFP Laser Wavelength</td>
<td>Specifies the laser wavelength of the installed pluggable transceiver.</td>
</tr>
<tr>
<td>Datecode</td>
<td>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 &quot;How To Troubleshoot Fiber and Pluggable Issues&quot; in the &quot;Getting Started with AlliedWare Plus&quot; Feature Overview and Configuration Guide.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Specifies the device type for the installed pluggable transceiver.</td>
</tr>
</tbody>
</table>
SHOW SYSTEM PLUGGABLE

Related Commands

- show system environment
- show system pluggable detail
- show system pluggable diagnostics
show system pluggable detail

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  

```
show system pluggable [port-list] detail
```

**Parameter**  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports to display information about. The port list can be:</td>
</tr>
<tr>
<td></td>
<td>• a switch port (e.g. port1.0.12)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.24</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of ports and port ranges, e.g. port1.0.1, port1.0.4-1.2.24</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Usage**  For a stacked configuration, if this command is entered on the stack master, it will display detailed information about the pluggable transceivers for all the stack members. A stack member heading will be displayed to distinguish the different pluggable transceiver information for every stack member.

**NOTE:**

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 (62.5 μm) Fiber**: Specifies the link length (in μm - micron) supported by the pluggable transceiver using 62.5 micron multi-mode fiber.
- **OM2 (50 μm) Fiber**: Specifies the link length (in μm - micron) supported by the pluggable transceiver using 50 micron multi-mode fiber.
- **Diagnostic Calibration**: Specifies whether the pluggable transceiver supports DDM or DOM Internal or External Calibration.
  - **Internal** is displayed if the pluggable transceiver supports DDM or DOM Internal Calibration.
  - **External** is displayed if the pluggable transceiver supports DDM or DOM External Calibration.
  - `-` is displayed if SFP or SFP+ DDM Internal Calibration or External Calibration is not supported.
- **Power Monitoring**: Displays the received power measurement type, which can be either **OMA** (Optical Module Amplitude) or **Avg** (Average Power) measured in 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 port1.0.24 detail
```

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

```
awplus# show system pluggable detail
```
Output  Figure 5-27: Example output from the show system pluggable detail command on a device

```
awplus#show system pluggable port1.0.24 detail
System Pluggable Information Detail

Port1.0.24

-------------
Vendor Name:              AGILENT
Device Name:              HFCT-5710L
Device Type:              1000BASE-LX
Serial Number:            0402142241184360
Manufacturing Datecode:   040214
SFP Laser Wavelength:     -
Link Length Supported
  Single Mode Fiber :     10Km
  OM1 (62.5um) Fiber:     550m
  OM2 (50um) Fiber :     550m
Diagnostic Calibration:   Internal
Power Monitoring:         Avg
FEC BER support:          -
```

Example  To display detailed information about the pluggable transceivers installed on a stack, use the command:

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

Figure 5-28: Example output from the `show system pluggable detail` command on a stack

```
awplus#show system pluggable detail
System Pluggable Information Detail

Stack member 1:
Port1.0.24
---------
Vendor Name: AGILENT
Device Name: HFCT-5710L
Device Type: 1000BASE-LX
Serial Number: 0402142241184360
Manufacturing Datecode: 040214
SFP Laser Wavelength: -
Link Length Supported
  Single Mode Fiber : 10Km
  OM1 (62.5um) Fiber: 550m
  OM2 (50um) Fiber : 550m
Diagnostic Calibration: Internal
Power Monitoring: Avg
FEC BER support: -

Stack member 2:
Port2.0.24
---------
Vendor Name: FINISAR CORP.
Device Name: FTRJ-8519-7D-CSC
Device Type: 1000BASE-SX
Serial Number: P430KGY
Manufacturing Datecode: 030718
SFP Laser Wavelength: 850nm
Link Length Supported
  Single Mode Fiber : -
  OM1 (62.5um) Fiber: 300m
  OM2 (50um) Fiber : 550m
Diagnostic Calibration: Internal
Power Monitoring: OMA
FEC BER support: Yes
```

Table 5-8: Parameters in the output from the `show system pluggables detail` command:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack member</td>
<td>The stack member number..</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port the pluggable transceiver is installed in.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Specifies the vendor’s name for the installed pluggable transceiver.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Specifies the device name for the installed pluggable transceiver.</td>
</tr>
</tbody>
</table>
### SYSTEM CONFIGURATION AND MONITORING COMMANDS

**SHOW SYSTEM PLUGGABLE DETAIL**

#### Related Commands
- show system environment
- show system pluggable
- show system pluggable diagnostics

#### Table 5-8: Parameters in the output from the `show system pluggable detail` command: (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>Specifies the device type for the installed pluggable transceiver.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Specifies the serial number for the installed pluggable transceiver.</td>
</tr>
<tr>
<td>Manufacturing Datecode</td>
<td>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 &quot;How To Troubleshoot Fiber and Pluggable Issues&quot; in the &quot;Getting Started with AlliedWare Plus&quot; Feature Overview and Configuration Guide.</td>
</tr>
<tr>
<td>SFP Laser Wavelength</td>
<td>Specifies the laser wavelength of the installed pluggable transceiver.</td>
</tr>
<tr>
<td>Single Mode Fiber</td>
<td>Specifies the link length supported by the pluggable transceiver using single mode fiber.</td>
</tr>
<tr>
<td>OM1 (62.5um) Fiber</td>
<td>Specifies the link length (in μm - micron) supported by the pluggable transceiver using 62.5 micron multi-mode fiber.</td>
</tr>
<tr>
<td>OM2 (50um) Fiber</td>
<td>Specifies the link length (in μm - micron) supported by the pluggable transceiver using 50 micron multi-mode fiber.</td>
</tr>
<tr>
<td>Diagnostic Calibration</td>
<td>Specifies whether the pluggable transceiver supports DDM or DOM Internal or External Calibration: <strong>Internal</strong> is displayed if the pluggable transceiver supports DDM or DOM Internal Calibration. <strong>External</strong> is displayed if the pluggable transceiver supports DDM or DOM External Calibration. - is displayed if SFP or SFP+ DDM Internal Calibration or External Calibration is not supported.</td>
</tr>
<tr>
<td>Power Monitoring</td>
<td>Displays the received power measurement type, which can be either <strong>OMA</strong> (Optical Module Amplitude) or <strong>Avg</strong> (Average Power) measured in μW.</td>
</tr>
</tbody>
</table>
show system pluggable diagnostics

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

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

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

**Mode**
User Exec and Privileged Exec

**Usage**
For a stacked configuration, if this command is entered on the stack master, it will display information about the pluggable transceivers for all the stack members. A stack member heading will be displayed to distinguish different pluggable transceiver information for every stack member.

Modern optical SFP and SFP+ transceivers support Digital Diagnostics Monitoring (DDM) functions.

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

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

awplus# show system pluggable diagnostics
**Output**  Figure 5-29: Example output from the `show system pluggable diagnostics` command on a device

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

<table>
<thead>
<tr>
<th>Port 1.0.21</th>
<th>Status</th>
<th>Alarms</th>
<th>Warnings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reading</td>
<td>Alarm</td>
<td>Max</td>
</tr>
<tr>
<td>Temp: (Degrees C)</td>
<td>29.387</td>
<td>- 100.00</td>
<td>-40.00</td>
</tr>
<tr>
<td>Vcc: (Volts)</td>
<td>3.339</td>
<td>- 3.465</td>
<td>3.135</td>
</tr>
<tr>
<td>Tx Bias: (mA)</td>
<td>10.192</td>
<td>- 37.020</td>
<td>3.260</td>
</tr>
<tr>
<td>Tx Power: (mW)</td>
<td>17.872</td>
<td>- 35.643</td>
<td>8.953</td>
</tr>
<tr>
<td>Rx Power: (mW)</td>
<td>0.006</td>
<td>Low 15.849</td>
<td>0.025</td>
</tr>
<tr>
<td>Rx LOS:</td>
<td>Rx Down</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port 1.0.22</th>
<th>Status</th>
<th>Alarms</th>
<th>Warnings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reading</td>
<td>Alarm</td>
<td>Max</td>
</tr>
<tr>
<td>Temp: (Degrees C)</td>
<td>29.387</td>
<td>- 100.00</td>
<td>-40.00</td>
</tr>
<tr>
<td>Vcc: (Volts)</td>
<td>3.378</td>
<td>- 3.630</td>
<td>2.970</td>
</tr>
<tr>
<td>Tx Bias: (mA)</td>
<td>2.802</td>
<td>- 6.000</td>
<td>1.000</td>
</tr>
<tr>
<td>Tx Power: (mW)</td>
<td>2.900</td>
<td>- 11.000</td>
<td>0.600</td>
</tr>
<tr>
<td>Rx Power: (mW)</td>
<td>1.739</td>
<td>- 18.000</td>
<td>0.000</td>
</tr>
<tr>
<td>Rx LOS:</td>
<td>Rx Up</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Output**  Figure 5-30: Example output from the `show system pluggable diagnostics port1.0.22` command on a switch

```
awplus#show system pluggable port1.0.22 diagnostics
System Pluggable Information Diagnostics

<table>
<thead>
<tr>
<th>Port 1.0.22</th>
<th>Status</th>
<th>Alarms</th>
<th>Warnings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reading</td>
<td>Alarm</td>
<td>Max</td>
</tr>
<tr>
<td>Temp: (Degrees C)</td>
<td>29.387</td>
<td>- 100.00</td>
<td>-40.00</td>
</tr>
<tr>
<td>Vcc: (Volts)</td>
<td>3.378</td>
<td>- 3.630</td>
<td>2.970</td>
</tr>
<tr>
<td>Tx Bias: (mA)</td>
<td>2.802</td>
<td>- 6.000</td>
<td>1.000</td>
</tr>
<tr>
<td>Tx Power: (mW)</td>
<td>2.900</td>
<td>- 11.000</td>
<td>0.600</td>
</tr>
<tr>
<td>Rx Power: (mW)</td>
<td>1.739</td>
<td>- 18.000</td>
<td>0.000</td>
</tr>
<tr>
<td>Rx LOS:</td>
<td>Rx Up</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Table 5-9:** Parameters in the output from the `show system pluggables diagnostics` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp (Degrees C)</td>
<td>Shows the temperature inside the transceiver.</td>
</tr>
<tr>
<td>Vcc (Volts)</td>
<td>Shows voltage supplied to the transceiver.</td>
</tr>
<tr>
<td>Tx Bias (mA)</td>
<td>Shows current to the Laser Diode in the transceiver.</td>
</tr>
</tbody>
</table>
### Table 5-9: Parameters in the output from the `show system pluggables diagnostics` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Power (mW)</td>
<td>Shows the amount of light transmitted from the transceiver.</td>
</tr>
<tr>
<td>Rx Power (mW)</td>
<td>Shows the amount of light received in the transceiver.</td>
</tr>
<tr>
<td>Rx LOS</td>
<td>Shows when the received optical level falls below a preset threshold.</td>
</tr>
</tbody>
</table>

**Related Commands**
- `show system environment`
- `show system pluggable`
- `show system pluggable detail`
**show system serialnumber**

**Overview**  This command shows the serial number information for the device.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show system serialnumber

**Mode**  User Exec and Privileged Exec

**Example**  To display the serial number information for the device, use the command:

```
awplus# show system serialnumber
```

**Output**  Figure 5-31:  Example output from the *show system serial number* command

```
awplus#show system serialnumber
45AX5300X
```
show tech-support

**Overview**  This command generates system and debugging information for the device and saves it to a file. You can optionally limit the command output to display only information for a given protocol or feature.

The command generates a large amount of output, which is saved to a file in compressed format. The output file name can be specified by outfile option. If the output file already exists, a new file name is generated with the current time stamp. If the output filename does not end with “.gz”, then “.gz” is appended to the filename. Since output files may be too large for Flash on the device we recommend saving files to external memory or a TFTP server whenever possible to avoid device lockup. This method is not likely to be appropriate when running the working set option of AMF across a range of physically separated devices.

**Syntax**  

```
show tech-support {all| [atmf|dhcpsn|epsr|igmp|ip|ipv6|mld|ospf|ospf6|pim|rip|ripng|stack|stp|system|tacacs+]| [outfile <filename> ]}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Display full information</td>
</tr>
<tr>
<td>atmf</td>
<td>Display ATMF- specific information</td>
</tr>
<tr>
<td>dhcpsn</td>
<td>Display DHCP Snooping specific information</td>
</tr>
<tr>
<td>epsr</td>
<td>Display EPSR specific information</td>
</tr>
<tr>
<td>igmp</td>
<td>Display IGMP specific information</td>
</tr>
<tr>
<td>ip</td>
<td>Display IP specific information</td>
</tr>
<tr>
<td>ipv6</td>
<td>Display IPv6 specific information</td>
</tr>
<tr>
<td>mld</td>
<td>Display MLD specific information</td>
</tr>
<tr>
<td>ospf</td>
<td>Display OSPF related information</td>
</tr>
<tr>
<td>ospf6</td>
<td>Display OSPF6 specific information</td>
</tr>
<tr>
<td>outfile</td>
<td>Output file name</td>
</tr>
<tr>
<td>pim</td>
<td>Display PIM related information</td>
</tr>
<tr>
<td>rip</td>
<td>RIP related information</td>
</tr>
<tr>
<td>ripng</td>
<td>Display RIPNG specific information</td>
</tr>
<tr>
<td>stack</td>
<td>Display stacking device information</td>
</tr>
<tr>
<td>stp</td>
<td>Display STP specific information</td>
</tr>
<tr>
<td>system</td>
<td>Display general system information</td>
</tr>
<tr>
<td>tacacs+</td>
<td>Display TACACS+ information</td>
</tr>
<tr>
<td></td>
<td>Output modifier</td>
</tr>
<tr>
<td>&gt;</td>
<td>Output redirection</td>
</tr>
</tbody>
</table>
Default  Captures all information for the device.

By default the output is saved to the file ‘tech-support.txt.gz’ in the current directory. If this file already exists in the current directory then a new file is generated with the time stamp appended to the file name, for example ‘tech-support20080109.txt.gz’, so the last saved file is retained.

Usage  This command is useful for collecting a large amount of information about all protocols or specific protocols on your device so that it can then be analyzed for troubleshooting purposes. The output of this command can be provided to technical support staff when reporting a problem.

Mode  Privileged Exec

Examples  show tech-support

awplus# show tech-support

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;&gt;</td>
<td>Output redirection (append)</td>
</tr>
<tr>
<td>&lt;filename&gt;</td>
<td>Specifies a name for the output file. If no name is specified, this file will be saved as: tech-support.txt.gz.</td>
</tr>
</tbody>
</table>
**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>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;console-speed-in-bps&gt;</code></td>
<td>Console speed Baud rate in bps (bits per second).</td>
</tr>
<tr>
<td>1200</td>
<td>1200 Baud</td>
</tr>
<tr>
<td>2400</td>
<td>2400 Baud</td>
</tr>
<tr>
<td>9600</td>
<td>9600 Baud</td>
</tr>
<tr>
<td>19200</td>
<td>19200 Baud</td>
</tr>
<tr>
<td>38400</td>
<td>38400 Baud</td>
</tr>
<tr>
<td>57600</td>
<td>57600 Baud</td>
</tr>
<tr>
<td>115200</td>
<td>115200 Baud</td>
</tr>
</tbody>
</table>

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

**Mode**  Line Configuration

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

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

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

Then log in again to enable the change:

```
awplus login:
Password:
awplus>
```
Related Commands

- clear line console
- line
- show running-config
- show startup-config
- speed
**system territory (deprecated)**

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

**Overview**
Use this command to display debugging output on a terminal.

To display the cursor after a line of debugging output, press the Enter key.

Use the command `terminal no monitor` to stop displaying debugging output on the terminal, or use the timeout option to stop displaying debugging output on the terminal after a set time.

**Syntax**
terminal monitor [<1-60>]
terminal no monitor

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-60&gt;</td>
<td>Set a timeout between 1 and 60 seconds for terminal output.</td>
</tr>
</tbody>
</table>

**Default**
Disabled

**Mode**
User Exec and Privileged Exec

**Examples**
To display debugging output on a terminal, enter the command:
awplus# terminal monitor

To specify timeout of debugging output after 60 seconds, enter the command:
awplus# terminal monitor 60

To stop displaying debugging output on the terminal, use the command:
awplus# terminal no monitor

**Related Commands**
All debug commands
**Overview**  This command applies the functionality of the no debug all command.
6 Logging Commands

Introduction

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

Command List
- “clear exception log” on page 298
- “clear log” on page 299
- “clear log buffered” on page 300
- “clear log permanent” on page 301
- “default log buffered” on page 302
- “default log console” on page 303
- “default log email” on page 304
- “default log host” on page 305
- “default log monitor” on page 306
- “default log permanent” on page 307
- “exception coredump size (deleted)” on page 308
- “log buffered” on page 309
- “log buffered (filter)” on page 310
- “log buffered size” on page 313
- “log console” on page 314
- “log console (filter)” on page 315
- “log email” on page 318
- “log email (filter)” on page 319
- “log email time” on page 323
- “log host” on page 325
- “log host (filter)” on page 326
- “log host time” on page 330
- “log monitor (filter)” on page 332
- “log permanent” on page 335
- “log permanent (filter)” on page 336
- “log permanent size” on page 339
- “log-rate-limit nsm” on page 340
- “show counter log” on page 342
- “show exception log” on page 343
- “show log” on page 344
- “show log config” on page 347
- “show log permanent” on page 350
- “show running-config log” on page 351
**clear exception log**

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

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

**Syntax**  clear exception log

**Mode**  Privileged Exec

**Example**  awplus# clear exception log
clear log

**Overview**  This command removes the contents of the buffered and permanent logs.

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

**Syntax**  clear log

**Mode**  Privileged Exec

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

```plaintext
awplus# clear log
```

**Validation Commands**  show log

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

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

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

**Syntax**  clear log buffered

**Mode**  Privileged Exec

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

```
awplus# clear log buffered
```

**Validation Commands**  show log

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

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

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

**Syntax**  clear log permanent

**Mode**  Privileged Exec

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

```
awplus# clear log permanent
```

**Validation Commands**  show log

**Related Commands**  clear log
clear log buffered
**default log buffered**

**Overview**  
This command restores the default settings for the buffered log stored in RAM. By default the size of the buffered log is 50 kB and it accepts messages with the severity level of “warnings” and above.

**Syntax**  
default log buffered

**Default**  
The buffered log is enabled by default.

**Mode**  
Global Configuration

**Example**  
To restore the buffered log to its default settings use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# default log buffered
```

**Validation Commands**  
show log config

**Related Commands**  
log buffered  
log buffered size
default log console

Overview
This command restores the default settings for log messages sent to the terminal when a log console command is issued. By default all messages are sent to the console when a log console command is issued.

Syntax
default log console

Mode
Global Configuration

Example
To restore the log console to its default settings use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# default log console
```

Validation
Commands
show log config

Related Commands
log console
log console (filter)
default log email

Overview  This command restores the default settings for log messages sent to an email address. By default no filters are defined for email addresses. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

Syntax  default log email <email-address>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;email-address&gt;</td>
<td>The email address to send log messages to</td>
</tr>
</tbody>
</table>

Mode  Global Configuration

Example  To restore the default settings for log messages sent to the email address admin@alliedtelesis.com use the following commands:

```
awplus# configure terminal
awplus(config)# default log email admin@alliedtelesis.com
```

Related Commands  show log config
**default log host**

**Overview**
This command restores the default settings for log sent to a remote syslog server. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

**Syntax**
default log host <ip-addr>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of a remote syslog server</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Example**
To restore the default settings for messages sent to the remote syslog server with IP address 10.32.16.21 use the following commands:

```
awplus# configure terminal
awplus(config)# default log host 10.32.16.21
```

**Validation Commands**
show log config

**Related Commands**
log email
**default log monitor**

**Overview**  This command restores the default settings for log messages sent to the terminal when a `terminal monitor` command is used.

**Syntax**  `default log monitor`

**Default**  All messages are sent to the terminal when a `terminal monitor` command is used.

**Mode**  Global Configuration

**Example**  To restore the log monitor to its default settings use the following commands:
```
awplus# configure terminal
awplus(config)# default log monitor
```

**Related Commands**  
- `log monitor (filter)`
- `show log config`
default log permanent

**Overview**  This command restores the default settings for the permanent log stored in NVS. By default, the size of the permanent log is 50 kB and it accepts messages with the severity level of `warnings` and above.

**Syntax**  `default log permanent`

**Default**  The permanent log is enabled by default.

**Mode**  Global Configuration

**Example**  To restore the permanent log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log permanent
```

**Related Commands**  
- `log permanent`
- `log permanent size`
- `show log config`
exception coredump size (deleted)

**Overview**  This command has been deprecated in the 5.4.4 software version, and deleted in the 5.4.4-1.1 version. There are no alternative commands.
**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 configure the device to store log messages in RAM use the following commands:
```
awplus# configure terminal
awplus(config)# log buffered
```

To configure the device to not store log messages in a RAM buffer use the following commands:
```
awplus# configure terminal
awplus(config)# no log buffered
```

**Validation Commands**
```
show log config
```

**Related Commands**
```
default log buffered
log buffered (filter)
log buffered size
```
**LOGGING COMMANDS**

**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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>Filter messages to the buffered log by severity level.</td>
</tr>
<tr>
<td>&lt;level&gt;</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>7</td>
</tr>
<tr>
<td>program</td>
<td>Filter messages to the buffered log by program. Include messages from a specified program in the buffered log.</td>
</tr>
</tbody>
</table>
**LOGGING COMMANDS**

**LOG BUFFERED (FILTER)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;program-name&gt;</code></td>
<td>The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:</td>
</tr>
<tr>
<td>rip</td>
<td>Routing Information Protocol (RIP)</td>
</tr>
<tr>
<td>ripng</td>
<td>Routing Information Protocol - next generation (RIPng)</td>
</tr>
<tr>
<td>ospf</td>
<td>Open Shortest Path First (OSPF)</td>
</tr>
<tr>
<td>ospfv3</td>
<td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td>
</tr>
<tr>
<td>rsvp</td>
<td>Resource Reservation Protocol (RSVP)</td>
</tr>
<tr>
<td>pim-dm</td>
<td>Protocol Independent Multicast - Dense Mode (PIM-DM)</td>
</tr>
<tr>
<td>pim-sm</td>
<td>Protocol Independent Multicast - Sparse Mode (PIM-SM)</td>
</tr>
<tr>
<td>pim-smv6</td>
<td>PIM-SM version 6 (PIM-SMv6)</td>
</tr>
<tr>
<td>dot1x</td>
<td>IEEE 802.1X Port-Based Access Control</td>
</tr>
<tr>
<td>lacp</td>
<td>Link Aggregation Control Protocol (LACP)</td>
</tr>
<tr>
<td>stp</td>
<td>Spanning Tree Protocol (STP)</td>
</tr>
<tr>
<td>rstp</td>
<td>Rapid Spanning Tree Protocol (RSTP)</td>
</tr>
<tr>
<td>mstp</td>
<td>Multiple Spanning Tree Protocol (MSTP)</td>
</tr>
<tr>
<td>imi</td>
<td>Integrated Management Interface (IMI)</td>
</tr>
<tr>
<td>imish</td>
<td>Integrated Management Interface Shell (IMISH)</td>
</tr>
<tr>
<td>epsr</td>
<td>Ethernet Protection Switched Rings (EPSR)</td>
</tr>
<tr>
<td>rmon</td>
<td>Remote Monitoring</td>
</tr>
<tr>
<td>loopprot</td>
<td>Loop Protection</td>
</tr>
<tr>
<td>poe</td>
<td>Power-inline (Power over Ethernet)</td>
</tr>
<tr>
<td>dhcpsn</td>
<td>DHCP snooping (DHCPsn)</td>
</tr>
</tbody>
</table>

Filter messages to the buffered log by syslog facility.

Specify one of the following syslog facilities to include messages from in the buffered log:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kern</td>
<td>Kernel messages</td>
</tr>
<tr>
<td>user</td>
<td>Random user-level messages</td>
</tr>
<tr>
<td>mail</td>
<td>Mail system</td>
</tr>
<tr>
<td>daemon</td>
<td>System daemons</td>
</tr>
<tr>
<td>auth</td>
<td>Security/authorization messages</td>
</tr>
<tr>
<td>syslog</td>
<td>Messages generated internally by syslogd</td>
</tr>
<tr>
<td>lpr</td>
<td>Line printer subsystem</td>
</tr>
<tr>
<td>news</td>
<td>Network news subsystem</td>
</tr>
<tr>
<td>uucp</td>
<td>UUCP subsystem</td>
</tr>
<tr>
<td>cron</td>
<td>Clock daemon</td>
</tr>
</tbody>
</table>
LOGGING COMMANDS

LOG BUFFERED (FILTER)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authpriv</td>
<td>Security/authorization messages (private)</td>
</tr>
<tr>
<td>ftp</td>
<td>FTP daemon</td>
</tr>
<tr>
<td>msgtext</td>
<td>Select messages containing a certain text string.</td>
</tr>
<tr>
<td>&lt;text-string&gt;</td>
<td>A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.</td>
</tr>
</tbody>
</table>

**Default**

By default the buffered log has a filter to select messages whose severity level is "notices (5)" or higher. This filter may be removed using the **no** variant of this command.

**Mode**

Global Configuration

**Examples**

To add a filter to send all messages generated by EPSR that have a severity of notices or higher to the buffered log use the following commands:

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

To add a filter to send all messages containing the text *Bridging initialization*, to the buffered log use the following commands:

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

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

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

To remove a filter that sends all messages containing the text *Bridging initialization*, to the buffered log use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered msgtext Bridging initialization
```

**Validation Commands**

`show log config`

**Related Commands**

`default log buffered`

`log buffered`

`log buffered size`
log buffered size

**Overview**
This command configures the amount of memory that the buffered log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

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

**Mode**
Global Configuration

**Example**
To allow the buffered log to use up to 100 kB of RAM use the following commands:
```
awplus# configure terminal
awplus(config)# log buffered size 100
```

**Validation Commands**
```
show log config
```

**Related Commands**
```
default log buffered
log buffered
```
log console

**Overview**  This command configures the device to send log messages to consoles. The console log is configured by default to send messages to the 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
```

**Validation Commands**  `show log config`

**Related Commands**

- `log console (filter)`
LOGGING COMMANDS
LOG CONSOLE (FILTER)

log console (filter)

**Overview**  This command creates a filter to select messages to be sent to all consoles when the log console command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

**Syntax**

```
log console [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]

no log console [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>Filter messages by severity level.</td>
</tr>
<tr>
<td>&lt;level&gt;</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>7</td>
</tr>
<tr>
<td>program</td>
<td>Filter messages by program. Include messages from a specified program.</td>
</tr>
</tbody>
</table>
LOGGING COMMANDS
LOG CONSOLE (FILTER)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;program-name&gt;facility&gt;</td>
<td>The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:</td>
</tr>
<tr>
<td>rip</td>
<td>Routing Information Protocol (RIP)</td>
</tr>
<tr>
<td>ripng</td>
<td>Routing Information Protocol - next generation (RIPng)</td>
</tr>
<tr>
<td>ospf</td>
<td>Open Shortest Path First (OSPF)</td>
</tr>
<tr>
<td>ospfv3</td>
<td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td>
</tr>
<tr>
<td>rsvp</td>
<td>Resource Reservation Protocol (RSVP)</td>
</tr>
<tr>
<td>pim-dm</td>
<td>Protocol Independent Multicast - Dense Mode (PIM-DM)</td>
</tr>
<tr>
<td>pim-sm</td>
<td>Protocol Independent Multicast - Sparse Mode (PIM-SM)</td>
</tr>
<tr>
<td>pim-smv6</td>
<td>PIM-SM version 6 (PIM-SMv6)</td>
</tr>
<tr>
<td>dot1x</td>
<td>IEEE 802.1X Port-Based Access Control</td>
</tr>
<tr>
<td>lacp</td>
<td>Link Aggregation Control Protocol (LACP)</td>
</tr>
<tr>
<td>stp</td>
<td>Spanning Tree Protocol (STP)</td>
</tr>
<tr>
<td>rstp</td>
<td>Rapid Spanning Tree Protocol (RSTP)</td>
</tr>
<tr>
<td>mstp</td>
<td>Multiple Spanning Tree Protocol (MSTP)</td>
</tr>
<tr>
<td>imi</td>
<td>Integrated Management Interface (IMI)</td>
</tr>
<tr>
<td>imish</td>
<td>Integrated Management Interface Shell (IMISH)</td>
</tr>
<tr>
<td>epsr</td>
<td>Ethernet Protection Switched Rings (EPSR)</td>
</tr>
<tr>
<td>rmon</td>
<td>Remote Monitoring</td>
</tr>
<tr>
<td>loopprot</td>
<td>Loop Protection</td>
</tr>
<tr>
<td>poe</td>
<td>Power-inline (Power over Ethernet)</td>
</tr>
<tr>
<td>dhcpsn</td>
<td>DHCP snooping (DHCPsn)</td>
</tr>
</tbody>
</table>

Filter messages by syslog facility.

Specify one of the following syslog facilities to include messages from:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kern</td>
<td>Kernel messages</td>
</tr>
<tr>
<td>user</td>
<td>Random user-level messages</td>
</tr>
<tr>
<td>mail</td>
<td>Mail system</td>
</tr>
<tr>
<td>daemon</td>
<td>System daemons</td>
</tr>
<tr>
<td>auth</td>
<td>Security/authorization messages</td>
</tr>
<tr>
<td>syslog</td>
<td>Messages generated internally by syslogd</td>
</tr>
<tr>
<td>lpr</td>
<td>Line printer subsystem</td>
</tr>
<tr>
<td>news</td>
<td>Network news subsystem</td>
</tr>
<tr>
<td>uucp</td>
<td>UUCP subsystem</td>
</tr>
<tr>
<td>cron</td>
<td>Clock daemon</td>
</tr>
</tbody>
</table>
LOGGING COMMANDS

LOG CONSOLE (FILTER)

Default
By default the buffered log has a filter to select messages whose severity level is critical or higher. This filter may be removed using the no variant of this command. This filter may be removed and replaced by filters that are more selective.

Mode
Global Configuration

Examples
To create a filter to send all messages generated by MSTP that have a severity of info or higher to console instances where the log console command has been given, remove the default filter that includes everything use the following commands:

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

and then use the command:

awplus(config)# log console level info program mstp

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

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

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

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

To remove a default filter that includes sending critical, alert and emergency level messages to the console use the following commands:

awplus# configure terminal
awplus(config)# no log console level critical

Validation
Commands
show log config

Related
Commands
log console

**Parameter** | **Description**
---|---
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.
**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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;email-address&gt;</code></td>
<td>The email address to send log messages to</td>
</tr>
</tbody>
</table>

**Default**  
By default no filters are defined for email log targets. Filters must be defined before messages will be sent.

**Mode**  
Global Configuration

**Example**  
To have log messages emailed to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com
```

**Validation Commands**  
```
show log config
```

**Related Commands**  
- `default log email`
- `log email`
LOGGING COMMANDS
LOG EMAIL (FILTER)

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**

```plaintext
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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;email-address&gt;</td>
<td>The email address to send logging messages to</td>
</tr>
<tr>
<td>level</td>
<td>Filter messages by severity level.</td>
</tr>
<tr>
<td>&lt;level&gt;</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>7</td>
</tr>
<tr>
<td>program</td>
<td>Filter messages by program. Include messages from a specified program.</td>
</tr>
</tbody>
</table>
## LOGGING COMMANDS

### LOG EMAIL (FILTER)

The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;program-name&gt;facility&lt;facility&gt;</td>
<td>The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:</td>
</tr>
<tr>
<td>rip</td>
<td>Routing Information Protocol (RIP)</td>
</tr>
<tr>
<td>ripng</td>
<td>Routing Information Protocol - next generation (RIPng)</td>
</tr>
<tr>
<td>ospf</td>
<td>Open Shortest Path First (OSPF)</td>
</tr>
<tr>
<td>ospfv3</td>
<td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td>
</tr>
<tr>
<td>rsvp</td>
<td>Resource Reservation Protocol (RSVP)</td>
</tr>
<tr>
<td>pim-dm</td>
<td>Protocol Independent Multicast - Dense Mode (PIM-DM)</td>
</tr>
<tr>
<td>pim-sm</td>
<td>Protocol Independent Multicast - Sparse Mode (PIM-SM)</td>
</tr>
<tr>
<td>pim-smv6</td>
<td>PIM-SM version 6 (PIM-SMv6)</td>
</tr>
<tr>
<td>dot1x</td>
<td>IEEE 802.1X Port-Based Access Control</td>
</tr>
<tr>
<td>lacp</td>
<td>Link Aggregation Control Protocol (LACP)</td>
</tr>
<tr>
<td>stp</td>
<td>Spanning Tree Protocol (STP)</td>
</tr>
<tr>
<td>rstp</td>
<td>Rapid Spanning Tree Protocol (RSTP)</td>
</tr>
<tr>
<td>mstp</td>
<td>Multiple Spanning Tree Protocol (MSTP)</td>
</tr>
<tr>
<td>imi</td>
<td>Integrated Management Interface (IMI)</td>
</tr>
<tr>
<td>imish</td>
<td>Integrated Management Interface Shell (IMISH)</td>
</tr>
<tr>
<td>epsr</td>
<td>Ethernet Protection Switched Rings (EPSR)</td>
</tr>
<tr>
<td>rmon</td>
<td>Remote Monitoring</td>
</tr>
<tr>
<td>looppot</td>
<td>Loop Protection</td>
</tr>
<tr>
<td>poe</td>
<td>Power-inline (Power over Ethernet)</td>
</tr>
<tr>
<td>dhcpsn</td>
<td>DHCP snooping (DHCPsN)</td>
</tr>
</tbody>
</table>

Filter messages by syslog facility.

Specify one of the following syslog facilities to include messages from:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kern</td>
<td>Kernel messages</td>
</tr>
<tr>
<td>user</td>
<td>Random user-level messages</td>
</tr>
<tr>
<td>mail</td>
<td>Mail system</td>
</tr>
<tr>
<td>daemon</td>
<td>System daemons</td>
</tr>
<tr>
<td>auth</td>
<td>Security/authorization messages</td>
</tr>
<tr>
<td>syslog</td>
<td>Messages generated internally by syslogd</td>
</tr>
<tr>
<td>lpr</td>
<td>Line printer subsystem</td>
</tr>
<tr>
<td>news</td>
<td>Network news subsystem</td>
</tr>
<tr>
<td>uucp</td>
<td>UUCP subsystem</td>
</tr>
<tr>
<td>cron</td>
<td>Clock daemon</td>
</tr>
</tbody>
</table>
LOGGING COMMANDS

LOG EMAIL (FILTER)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authpriv</td>
<td>Security/authorization messages (private)</td>
</tr>
<tr>
<td>ftp</td>
<td>FTP daemon</td>
</tr>
<tr>
<td>msgtext</td>
<td>Select messages containing a certain text string.</td>
</tr>
<tr>
<td>&lt;text-string&gt;</td>
<td>A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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:

```plaintext
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:

```plaintext
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:

```plaintext
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:

```plaintext
awplus# configure terminal
awplus(config)# no log email admin@homebase.com level notices program epsr
```
To remove a filter that sends messages with a severity level of informational and above to the email address admin@alliedtelesis.com use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@alliedtelesis.com level informational
```

**Related Commands**
- default log email
- log email
- show log config
log email time

**Overview**
This command configures the time used in messages sent to an email address. If the syslog server is in a different time zone to your device then the time offset can be configured using either the `utc-offset` parameter option keyword or the `local-offset` parameter option keyword, where `utc-offset` is the time difference from UTC (Universal Time, Coordinated) and `local-offset` is the difference from local time.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;email-address&gt;</code></td>
<td>The email address to send log messages to</td>
</tr>
<tr>
<td>time</td>
<td>Specify the time difference between the email recipient and the device you are configuring.</td>
</tr>
<tr>
<td>local</td>
<td>The device is in the same time zone as the email recipient</td>
</tr>
<tr>
<td>local-offset</td>
<td>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.</td>
</tr>
<tr>
<td>utc-offset</td>
<td>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.</td>
</tr>
<tr>
<td>plus</td>
<td>Negative offset (difference) from the device to the email recipient.</td>
</tr>
<tr>
<td>minus</td>
<td>Positive offset (difference) from the device to the email recipient.</td>
</tr>
<tr>
<td><code>&lt;0-24&gt;</code></td>
<td>World Time zone offset in hours</td>
</tr>
</tbody>
</table>

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

**Mode**
Global Configuration

**Usage**
Use the `local` option if the email recipient is in the same time zone as this device. Messages will display the time as on the local device when the message was generated.

Use the `offset` option if the email recipient is in a different time zone to this device. Specify the time offset of the email recipient in hours. Messages will display the time they were generated on this device but converted to the time zone of the email recipient.
**Examples**

To send messages to the email address test@home.com in the same time zone as the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local 0
```

To send messages to the email address admin@base.com with the time information converted to the time zone of the email recipient, which is 3 hours ahead of the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local-offset plus 3
```

To send messages to the email address user@remote.com with the time information converted to the time zone of the email recipient, which is 3 hours behind the device's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email user@remote.com time utc-offset minus 3
```

**Validation Commands**

`show log config`

**Related Commands**

`default log buffered`
**log host**

**Overview**  This command configures the device to send log messages to a remote syslog server via UDP port 514. The IP address of the remote server must be specified. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent.

**Syntax**  
log host <ip-addr>

no log host <ip-addr>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of a remote syslog server in dotted decimal format A.B.C.D</td>
</tr>
</tbody>
</table>

**Mode**  Global Configuration

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

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

To stop the device from sending log messages to the remote syslog server with IP address 10.32.16.99 use the following commands:

awplus# configure terminal
awplus(config)# no log host 10.32.16.99

**Validation Commands**  show log config

**Related Commands**  default log host
**log host (filter)**

**Overview**  This command creates a filter to select messages to be sent to a remote syslog server. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a substring within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a remote syslog server. The IP address of the syslog server must be specified. All configuration relating to this log target will be removed.

**Syntax**
```
log host <ip-addr> [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]
```
```
no log host <ip-addr> [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of a remote syslog server.</td>
</tr>
<tr>
<td>level</td>
<td>Filter messages by severity level.</td>
</tr>
<tr>
<td>&lt;level&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>0</td>
<td>emergencies</td>
</tr>
<tr>
<td>1</td>
<td>alerts</td>
</tr>
<tr>
<td>2</td>
<td>critical</td>
</tr>
<tr>
<td>3</td>
<td>errors</td>
</tr>
<tr>
<td>4</td>
<td>warnings</td>
</tr>
<tr>
<td>5</td>
<td>notices</td>
</tr>
<tr>
<td>6</td>
<td>informational</td>
</tr>
<tr>
<td>7</td>
<td>debugging</td>
</tr>
<tr>
<td>program</td>
<td>Filter messages by program. Include messages from a specified program.</td>
</tr>
</tbody>
</table>
**LOGGING COMMANDS**

### LOG HOST (FILTER)

The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;program-name&gt;</td>
<td>The name of a program to log messages from.</td>
</tr>
<tr>
<td>&lt;facility&gt;</td>
<td>The facility to filter messages by.</td>
</tr>
</tbody>
</table>

- **rip**: Routing Information Protocol (RIP)
- **ripng**: Routing Information Protocol - next generation (RIPng)
- **ospf**: Open Shortest Path First (OSPF)
- **ospfv3**: Open Shortest Path First (OSPF) version 3 (OSPFv3)
- **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-Sv6)
- **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)
- **matp**: Multiple Spanning Tree Protocol (MSTP)
- **imi**: Integrated Management Interface (IMI)
- **imish**: Integrated Management Interface Shell (IMISH)
- **epsr**: Ethernet Protection Switched Rings (EPSR)
- **rmon**: Remote Monitoring
- **loopprot**: Loop Protection
- **poe**: Power-inline (Power over Ethernet)
- **dhcpsn**: DHCP snooping (DHCPSN)

Filter messages by syslog facility.

Specify one of the following syslog facilities to include messages from:

- **kern**: Kernel messages
- **user**: Random user-level messages
- **mail**: Mail system
- **daemon**: System daemons
- **auth**: Security/authorization messages
- **syslog**: Messages generated internally by syslogd
- **lpr**: Line printer subsystem
- **news**: Network news subsystem
- **uucp**: UUCP subsystem
- **cron**: Clock daemon
**LOG HOST (FILTER)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authpriv</td>
<td>Security/authorization messages (private)</td>
</tr>
<tr>
<td>ftp</td>
<td>FTP daemon</td>
</tr>
<tr>
<td>msgtext</td>
<td>Select messages containing a certain text string.</td>
</tr>
<tr>
<td>(&lt;text-string&gt;)</td>
<td>A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.</td>
</tr>
</tbody>
</table>

**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:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.21 level informational
```
LOGGING COMMANDS
LOG HOST (FILTER)

Related Commands
default log host
show log config
log host time

**Overview**
This command configures the time used in messages sent to a remote syslog server. If the syslog server is in a different time zone to your device then the time offset can be configured using either the `utc-offset` parameter option keyword or the `local-offset` parameter option keyword, where `utc-offset` is the time difference from UTC (Universal Time, Coordinated) and `local-offset` is the difference from local time.

**Syntax**
```
log host <email-address> time {local|local-offset|utc-offset {plus|minus} <0-24>}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;email-address&gt;</code></td>
<td>The email address to send log messages to</td>
</tr>
<tr>
<td>time</td>
<td>Specify the time difference between the email recipient and the device you are configuring.</td>
</tr>
<tr>
<td>local</td>
<td>The device is in the same time zone as the email recipient</td>
</tr>
<tr>
<td>local-offset</td>
<td>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.</td>
</tr>
<tr>
<td>utc-offset</td>
<td>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.</td>
</tr>
<tr>
<td>plus</td>
<td>Negative offset (difference) from the device to the syslog server.</td>
</tr>
<tr>
<td>minus</td>
<td>Positive offset (difference) from the device to the syslog server.</td>
</tr>
<tr>
<td><code>&lt;0-24&gt;</code></td>
<td>World Time zone offset in hours</td>
</tr>
</tbody>
</table>

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

**Mode**
Global Configuration

**Usage**
Use the `local` option if the remote syslog server is in the same time zone as the device. Messages will display the time as on the local device when the message was generated.

Use the `offset` option if the email recipient is in a different time zone to this device. Specify the time offset of the remote syslog server in hours. Messages will display the time they were generated on this device but converted to the time zone of the remote syslog server.

**Examples**
To send messages to the remote syslog server with the IP address 10.32.16.21 in the same time zone as the device’s local time zone, use the following commands:

```bash
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:

```bash
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:

```bash
awplus# configure terminal
awplus(config)# log host 10.32.16.02 time utc-offset minus 3
```

Validation Commands
- `show log config`

Related Commands
- `default log buffered`
**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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>Filter messages by severity level.</td>
</tr>
<tr>
<td>&lt;level&gt;</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>7</td>
</tr>
<tr>
<td>program</td>
<td>Filter messages by program. Include messages from a specified program.</td>
</tr>
</tbody>
</table>
## LOGGING COMMANDS

### LOG MONITOR (FILTER)

The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rip</td>
<td>Routing Information Protocol (RIP)</td>
</tr>
<tr>
<td>ripng</td>
<td>Routing Information Protocol - next generation (RIPng)</td>
</tr>
<tr>
<td>ospf</td>
<td>Open Shortest Path First (OSPF)</td>
</tr>
<tr>
<td>ospfv3</td>
<td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td>
</tr>
<tr>
<td>rsvp</td>
<td>Resource Reservation Protocol (RSVP)</td>
</tr>
<tr>
<td>pim-dm</td>
<td>Protocol Independent Multicast - Dense Mode (PIM-DM)</td>
</tr>
<tr>
<td>pim-sm</td>
<td>Protocol Independent Multicast - Sparse Mode (PIM-SM)</td>
</tr>
<tr>
<td>pim-smv6</td>
<td>PIM-SM version 6 (PIM-SMv6)</td>
</tr>
<tr>
<td>dotlx</td>
<td>IEEE 802.1X Port-Based Access Control</td>
</tr>
<tr>
<td>lacp</td>
<td>Link Aggregation Control Protocol (LACP)</td>
</tr>
<tr>
<td>stp</td>
<td>Spanning Tree Protocol (STP)</td>
</tr>
<tr>
<td>rstp</td>
<td>Rapid Spanning Tree Protocol (RSTP)</td>
</tr>
<tr>
<td>mstp</td>
<td>Multiple Spanning Tree Protocol (MSTP)</td>
</tr>
<tr>
<td>imi</td>
<td>Integrated Management Interface (IMI)</td>
</tr>
<tr>
<td>imish</td>
<td>Integrated Management Interface Shell (IMISH)</td>
</tr>
<tr>
<td>epsr</td>
<td>Ethernet Protection Switched Rings (EPSR)</td>
</tr>
<tr>
<td>rmon</td>
<td>Remote Monitoring</td>
</tr>
<tr>
<td>loopprot</td>
<td>Loop Protection</td>
</tr>
<tr>
<td>poe</td>
<td>Power-inline (Power over Ethernet)</td>
</tr>
<tr>
<td>dhcpsn</td>
<td>DHCP snooping (DHCPsn)</td>
</tr>
</tbody>
</table>

Filter messages by syslog facility.

Specify one of the following syslog facilities to include messages from:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kern</td>
<td>Kernel messages</td>
</tr>
<tr>
<td>user</td>
<td>Random user-level messages</td>
</tr>
<tr>
<td>mail</td>
<td>Mail system</td>
</tr>
<tr>
<td>daemon</td>
<td>System daemons</td>
</tr>
<tr>
<td>auth</td>
<td>Security/authorization messages</td>
</tr>
<tr>
<td>syslog</td>
<td>Messages generated internally by syslogd</td>
</tr>
<tr>
<td>lpr</td>
<td>Line printer subsystem</td>
</tr>
<tr>
<td>news</td>
<td>Network news subsystem</td>
</tr>
<tr>
<td>uucp</td>
<td>UUCP subsystem</td>
</tr>
<tr>
<td>cron</td>
<td>Clock daemon</td>
</tr>
</tbody>
</table>
### LOG MONITOR (FILTER)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authpriv</td>
<td>Security/authorization messages (private)</td>
</tr>
<tr>
<td>ftp</td>
<td>FTP daemon</td>
</tr>
<tr>
<td>msgtext</td>
<td>Select messages containing a certain text string.</td>
</tr>
<tr>
<td>&lt;text-string&gt;</td>
<td>A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.</td>
</tr>
</tbody>
</table>

**Default**  
By default there is a filter to select all messages. This filter may be removed and replaced by filters that are more selective.

**Mode**  
Global Configuration

**Examples**  
To create a filter to send all messages generated by MSTP that have a severity of info or higher to terminal instances where the terminal monitor command has been given use the following commands:

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

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

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

To remove a default filter that includes sending everything to the terminal use the following commands:

```
awplus# configure terminal
awplus(config)# no log monitor level debugging
```

**Validation Commands**  
`show log config`

**Related Commands**  
terminal monitor
**LOGGING COMMANDS**

**LOG PERMANENT**

---

**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
```

**Validation Commands**  `show log config`

**Related Commands**

- `default log permanent`
- `log permanent (filter)`
- `log permanent size`
- `show log permanent`
**log permanent (filter)**

**Overview**  This command creates a filter to select messages to be sent to the permanent log. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The `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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>level</strong></td>
<td>Filter messages sent to the permanent log by severity level.</td>
</tr>
<tr>
<td>&lt;level&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>0</td>
<td>emergencies</td>
</tr>
<tr>
<td>1</td>
<td>alerts</td>
</tr>
<tr>
<td>2</td>
<td>critical</td>
</tr>
<tr>
<td>3</td>
<td>errors</td>
</tr>
<tr>
<td>4</td>
<td>warnings</td>
</tr>
<tr>
<td>5</td>
<td>notices</td>
</tr>
<tr>
<td>6</td>
<td>informational</td>
</tr>
<tr>
<td>7</td>
<td>debugging</td>
</tr>
<tr>
<td><strong>program</strong></td>
<td>Filter messages by program. Include messages from a specified program.</td>
</tr>
</tbody>
</table>
### LOGGING COMMANDS

#### LOG PERMANENT (FILTER)

The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;program-name&gt;facilit&lt;facility&gt;</td>
<td>The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:</td>
</tr>
<tr>
<td>rip</td>
<td>Routing Information Protocol (RIP)</td>
</tr>
<tr>
<td>ripng</td>
<td>Routing Information Protocol - next generation (RIPng)</td>
</tr>
<tr>
<td>ospf</td>
<td>Open Shortest Path First (OSPF)</td>
</tr>
<tr>
<td>ospfv3</td>
<td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td>
</tr>
<tr>
<td>rsvp</td>
<td>Resource Reservation Protocol (RSVP)</td>
</tr>
<tr>
<td>pim-dm</td>
<td>Protocol Independent Multicast - Dense Mode (PIM-DM)</td>
</tr>
<tr>
<td>pim-sm</td>
<td>Protocol Independent Multicast - Sparse Mode (PIM-SM)</td>
</tr>
<tr>
<td>pim-smv6</td>
<td>PIM-SM version 6 (PIM-SMv6)</td>
</tr>
<tr>
<td>dot1x</td>
<td>IEEE 802.1X Port-Based Access Control</td>
</tr>
<tr>
<td>lacp</td>
<td>Link Aggregation Control Protocol (LACP)</td>
</tr>
<tr>
<td>stp</td>
<td>Spanning Tree Protocol (STP)</td>
</tr>
<tr>
<td>rstp</td>
<td>Rapid Spanning Tree Protocol (RSTP)</td>
</tr>
<tr>
<td>mstp</td>
<td>Multiple Spanning Tree Protocol (MSTP)</td>
</tr>
<tr>
<td>imi</td>
<td>Integrated Management Interface (IMI)</td>
</tr>
<tr>
<td>imish</td>
<td>Integrated Management Interface Shell (IMISH)</td>
</tr>
<tr>
<td>epsr</td>
<td>Ethernet Protection Switched Rings (EPSR)</td>
</tr>
<tr>
<td>rmon</td>
<td>Remote Monitoring</td>
</tr>
<tr>
<td>loopprot</td>
<td>Loop Protection</td>
</tr>
<tr>
<td>poe</td>
<td>Power-inline (Power over Ethernet)</td>
</tr>
<tr>
<td>dhcpsn</td>
<td>DHCP snooping (DHCPSN)</td>
</tr>
</tbody>
</table>

Filter messages by syslog facility.

Specify one of the following syslog facilities to include messages from:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kern</td>
<td>Kernel messages</td>
</tr>
<tr>
<td>user</td>
<td>Random user-level messages</td>
</tr>
<tr>
<td>mail</td>
<td>Mail system</td>
</tr>
<tr>
<td>daemon</td>
<td>System daemons</td>
</tr>
<tr>
<td>auth</td>
<td>Security/authorization messages</td>
</tr>
<tr>
<td>syslog</td>
<td>Messages generated internally by syslogd</td>
</tr>
<tr>
<td>lpr</td>
<td>Line printer subsystem</td>
</tr>
<tr>
<td>news</td>
<td>Network news subsystem</td>
</tr>
<tr>
<td>uucp</td>
<td>UUCP subsystem</td>
</tr>
<tr>
<td>cron</td>
<td>Clock daemon</td>
</tr>
</tbody>
</table>
### LOGGING COMMANDS

#### LOG PERMANENT (FILTER)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authpriv</td>
<td>Security/authorization messages (private)</td>
</tr>
<tr>
<td>ftp</td>
<td>FTP daemon</td>
</tr>
<tr>
<td>msgtext</td>
<td>Select messages containing a certain text string.</td>
</tr>
<tr>
<td>&lt;text-string&gt;</td>
<td>A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.</td>
</tr>
</tbody>
</table>

**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:

```bash
aplus# configure terminal
налus(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:

```bash
aplus# configure terminal
апlus(config)# log permanent msgtext Bridging initialization
```

**Validation Commands**

- `show log config`

**Related Commands**

- `default log permanent`
- `log permanent`
- `log permanent size`
- `show log permanent`
**log permanent size**

**Overview**  This command configures the amount of memory that the permanent log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

**Syntax**  

```
log permanent size <50-250>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;50-250&gt;</td>
<td>Size of the permanent log in kilobytes</td>
</tr>
</tbody>
</table>

**Mode**  Global Configuration

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

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

**Validation Commands**  `show log config`

**Related Commands**  `default log permanent`  `log permanent`
**Overview**  
This command limits the number of log messages generated by the device for a given interval.

Use the no variant of this command to revert to the default number of log messages generated by the device of up to 200 log messages per second.

**Syntax**
```
log-rate-limit nsm messages <message-limit> interval <time-interval>
no log-rate-limit nsm
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;message-limit&gt;</code></td>
<td>&lt;1-65535&gt; The number of log messages generated by the device.</td>
</tr>
<tr>
<td><code>&lt;time-interval&gt;</code></td>
<td>&lt;0-65535&gt; 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.</td>
</tr>
</tbody>
</table>

**Default**  
By default, the device will allow 200 log messages to be generated per second.

**Mode**  
Global Configuration

**Usage**  
Previously, if the device received a continuous stream of IGMP packets with errors, such as when a packet storm occurs because of a network loop, then the device generates a lot of log messages using more and more memory, which may ultimately cause the device to shutdown. This log rate limiting feature constrains the rate that log messages are generated by the device.

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

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

**Examples**  
To limit the device to generate up to 300 log messages per second, use the following commands:
```
awplus# configure terminal
awplus(config)# log-rate-limit nsm messages 300 interval 100
```
To return the device the default setting, to generate up to 200 log messages per second, use the following commands:

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

**Overview**  
This command displays log counter information.

**Syntax**  
`show counter log`

**Mode**  
User Exec and Privileged Exec

**Example**  
To display the log counter information, use the command:

```
awplus# show counter log
```

**Output**  
Figure 6-1: Example output from the `show counter log` command

<table>
<thead>
<tr>
<th>Log counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Received</td>
</tr>
<tr>
<td>Total Received P0</td>
</tr>
<tr>
<td>Total Received P1</td>
</tr>
<tr>
<td>Total Received P2</td>
</tr>
<tr>
<td>Total Received P3</td>
</tr>
<tr>
<td>Total Received P4</td>
</tr>
<tr>
<td>Total Received P5</td>
</tr>
<tr>
<td>Total Received P6</td>
</tr>
<tr>
<td>Total Received P7</td>
</tr>
</tbody>
</table>

Table 6-1: Parameters in output of the `show counter log` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Received</td>
<td>Total number of messages received by the log</td>
</tr>
<tr>
<td>Total Received P0</td>
<td>Total number of Priority 0 (Emergency) messages received</td>
</tr>
<tr>
<td>Total Received P1</td>
<td>Total number of Priority 1 (Alert) messages received</td>
</tr>
<tr>
<td>Total Received P2</td>
<td>Total number of Priority 2 (Critical) messages received</td>
</tr>
<tr>
<td>Total Received P3</td>
<td>Total number of Priority 3 (Error) messages received</td>
</tr>
<tr>
<td>Total Received P4</td>
<td>Total number of Priority 4 (Warning) messages received</td>
</tr>
<tr>
<td>Total Received P5</td>
<td>Total number of Priority 5 (Notice) messages received</td>
</tr>
<tr>
<td>Total Received P6</td>
<td>Total number of Priority 6 (Info) messages received</td>
</tr>
<tr>
<td>Total Received P7</td>
<td>Total number of Priority 7 (Debug) messages received</td>
</tr>
</tbody>
</table>

**Related Commands**  
`show log config`
**show exception log**

**Overview**  This command displays the contents of the exception log. When used within a stacked environment, this command will display the contents of the exception log for all the stack members.

**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 6-2: Example output from the `show exception log` command on a device

```
awplus# show exception log
Stack member 1:
<date> <time> <facility>.<severity> <program[pid]>: <message>
-------------------------------------------------------------------------
signal 11, core dumped to /flash/imish-x610-5.4.3-3.7-1-1390816667-3746.tgz
signal 11, core dumped to /flash/imish-x610-5.4.3-3.7-1-1390816667-2504.tgz
2014 Jan 27 09:58:02 local7.debug awplus corehandler : Process ospfd (PID:1512)
signal 5, core dumped to /flash/ospfd-x610-5.4.3-3.7-1-1390816682-1512.tgz
-------------------------------------------------------------------------
Stack member 2:
<date> <time> <facility>.<severity> <program[pid]>: <message>
-------------------------------------------------------------------------
signal 5, core dumped to /flash/imi-x610-5.4.3-3.7-2-1390816696-1427.tgz
-------------------------------------------------------------------------
```
show log

**Overview**  
This command displays the contents of the buffered log.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show log [tail [<10-250>]]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tail</td>
<td>Display only the latest log entries.</td>
</tr>
<tr>
<td>&lt;10-250&gt;</td>
<td>Specify the number of log entries to display.</td>
</tr>
</tbody>
</table>

**Default**  
By default the entire contents of the buffered log is displayed.

**Mode**  
User Exec, Privileged Exec and Global Configuration

**Usage**  
If the optional `tail` parameter is specified only the latest 10 messages in the buffered log are displayed. A numerical value can be specified after the `tail` parameter to select how many of the latest messages should be displayed.

**Examples**  
To display the contents of the buffered log use the command:

```
awplus# show log
```

To display the 10 latest entries in the buffered log use the command:

```
awplus# show log tail 10
```
LOGGING COMMANDS

SHOW LOG

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

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

2011 Aug 29 07:55:22 kern.notice awplus kernel: Linux version 2.6.32.12-at1 (maker@awpmaker03-dl) (gcc version 4.3.3 (Gentoo 4.3.3-r3 p1.2, p1e-10.1.5) ) #1 Wed Dec 8 11:53:40 NZDT 2010
2011 Aug 29 07:55:22 kern.warning awplus kernel: No pci config register base in dev tree, using default
2011 Aug 29 07:55:23 kern.notice awplus kernel: Kernel command line: console=ttys0,9600 releasefile=x510-5.4.5-0.1.rel ramdisk=14688
   bootversion=1.1.0-rc12 loglevel=1
   extraflash=00000000
2011 Aug 29 07:55:25 kern.notice awplus kernel: RAMDISK: squashfs filesystem found at block 0
.
.
.
```
Figure 6-4: Example output from the `show log tail` command

```
awplus#show log tail
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
--------------------------------------------------------------------
2006 Nov 10 13:30:01 cron.notice crond[116]: USER manager pid 469 cmd logrotate /etc/logrotate.conf
2006 Nov 10 13:30:01 cron.notice crond[116]: USER manager pid 471 cmd nbqueue -- wipe
2006 Nov 10 13:35:01 cron.notice crond[116]: USER manager pid 472 cmd nbqueue -- wipe
2006 Nov 10 13:40:01 cron.notice crond[116]: USER manager pid 477 cmd nbqueue -- wipe
2006 Nov 10 13:44:36 syslog.notice syslog-ng[67]: Log statistics; processed='center(queued)=70', processed='center(queued)=70'
2006 Nov 10 13:45:01 cron.notice crond[116]: USER manager pid 478 cmd logrotate /etc/logrotate.conf
2006 Nov 10 13:45:01 cron.notice crond[116]: USER manager pid 480 cmd nbqueue -- wipe
2006 Nov 10 13:49:32 syslog.notice syslog-ng[67]: SIGHUP received, reloading configuration;
2006 Nov 10 13:50:01 cron.notice crond[116]: USER manager pid 482 cmd nbqueue -- wipe
2006 Nov 10 13:55:01 cron.notice crond[116]: USER manager pid 483 cmd nbqueue -- wipe
.  
.  
```

**Related Commands**

- `show log config`
- `show log permanent`
show log config

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

**Syntax**  show log config

**Mode**  User Exec, Privileged Exec and Global Configuration

**Example**  To display the logging configuration use the command:

`awplus# show log config`
LOGGING COMMANDS
SHOW LOG CONFIG

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

<table>
<thead>
<tr>
<th>Buffered log:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status .......... enabled</td>
</tr>
<tr>
<td>Maximum size ... 100kb</td>
</tr>
<tr>
<td>Filters:</td>
</tr>
<tr>
<td>*1 Level ........ notices</td>
</tr>
<tr>
<td>Program ...... any</td>
</tr>
<tr>
<td>Facility ...... any</td>
</tr>
<tr>
<td>Message text . any</td>
</tr>
<tr>
<td>2 Level ........ informational</td>
</tr>
<tr>
<td>Program ...... mstp</td>
</tr>
<tr>
<td>Facility ...... daemon</td>
</tr>
<tr>
<td>Message text . any</td>
</tr>
<tr>
<td>Statistics ..... 1327 messages received, 821 accepted by filter (2006 Dec 11 10:36:16)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permanent log:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status .......... enabled</td>
</tr>
<tr>
<td>Maximum size ... 60kb</td>
</tr>
<tr>
<td>Filters:</td>
</tr>
<tr>
<td>1 Level ........ error</td>
</tr>
<tr>
<td>Program ...... any</td>
</tr>
<tr>
<td>Facility ...... any</td>
</tr>
<tr>
<td>Message text . any</td>
</tr>
<tr>
<td>*2 Level ........ warnings</td>
</tr>
<tr>
<td>Program ...... dhcp</td>
</tr>
<tr>
<td>Facility ...... any</td>
</tr>
<tr>
<td>Message text . &quot;pool exhausted&quot;</td>
</tr>
<tr>
<td>Statistics ..... 1327 messages received, 12 accepted by filter (2006 Dec 11 10:36:16)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Host 10.32.16.21:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time offset .... +2:00</td>
</tr>
<tr>
<td>Offset type .... UTC</td>
</tr>
<tr>
<td>Filters:</td>
</tr>
<tr>
<td>1 Level ........ critical</td>
</tr>
<tr>
<td>Program ...... any</td>
</tr>
<tr>
<td>Facility ...... any</td>
</tr>
<tr>
<td>Message text . any</td>
</tr>
<tr>
<td>Statistics ..... 1327 messages received, 1 accepted by filter (2006 Dec 11 10:36:16)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email <a href="mailto:admin@alliedtelesis.com">admin@alliedtelesis.com</a>:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time offset .... +0:00</td>
</tr>
<tr>
<td>Offset type .... Local</td>
</tr>
<tr>
<td>Filters:</td>
</tr>
<tr>
<td>1 Level ........ emergencies</td>
</tr>
<tr>
<td>Program ...... any</td>
</tr>
<tr>
<td>Facility ...... any</td>
</tr>
<tr>
<td>Message text . any</td>
</tr>
<tr>
<td>Statistics ..... 1327 messages received, 0 accepted by filter (2006 Dec 11 10:36:16)</td>
</tr>
</tbody>
</table>

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.
LOGGING COMMANDS
SHOW LOG CONFIG

Related Commands
show counter log
show log
show log permanent
show log permanent

**Overview**  This command displays the contents of the permanent log.
When used within a stacked environment, this command will display the contents of the permanent log for all the stack members, unless you specify a particular stack member.

**Syntax**  `show log permanent[<stack-ID>][tail [<10-250>]]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;stack-ID&gt;</code></td>
<td>Stack member number, from 1 to 8.</td>
</tr>
<tr>
<td><code>tail</code></td>
<td>Display only the latest log entries.</td>
</tr>
<tr>
<td><code>&lt;10-250&gt;</code></td>
<td>Specify the number of log entries to display.</td>
</tr>
</tbody>
</table>

**Default**  If the optional `tail` parameter is specified only the latest 10 messages in the permanent log are displayed. A numerical value can be specified after the `tail` parameter to select how many of the latest messages should be displayed.

**Mode**  User Exec, Privileged Exec and Global Configuration

**Example**  To display the permanent log of stack member 2, use the command:

```
awplus# show log permanent 2
```

**Output**

```
awplus# show log permanent 2
Stack member 2:
<date> <time> <facility>.<severity> <program>[<pid>]: <message>
-------------------------------------------------------------------------
2014 Feb 25 09:10:48 daemon.crit awplus-2 HPI: HOTSWAP Pluggable 2.0.51 hotswapped in: AT-StackXS/1.0
2014 Feb 25 09:10:50 user.crit awplus-2 VCS[922]: Member 1 (eccd.6d7d.a50e) has joined the stack
2014 Feb 25 09:10:52 user.crit awplus-2 VCS[922]: Member 1 (eccd.6d7d.a50e) has become the Active Master
2014 Feb 25 09:10:52 local6.alert awplus-2 VCS[922]: Stack member has booted from non-default location, SW version auto synchronization cannot be supported.
2014 Feb 25 09:10:52 user.crit awplus-2 VCS[922]: Stack Virtual MAC is 0000.cd37.0002
2014 Feb 25 09:11:46 user.crit awplus-2 ATMF[862]: awplus-x510 has joined. 1 member in total.
```

**Related Commands**  `show log`
show running-config log

**Overview**  
This command displays the current running configuration of the Log utility.

**Syntax**  
show running-config log

**Mode**  
Privileged Exec and Global Configuration

**Example**  
To display the current configuration of the log utility, use the command:

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

**Related Commands**  
show log
show log config
Scripting Commands

Introduction

Overview  This chapter provides commands used for command scripts.

Command List
- “activate” on page 352
- “echo” on page 353
- “wait” on page 354
activate

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>background</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;script&gt;</td>
<td>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 <code>.scp</code> or a <code>.sh</code> filename extension for a valid script text file, as described below in the usage section for this command.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Usage**
When a script is activated, the privilege level is set to 1 enabling User Exec commands to run in the script. If you need to run Privileged Exec commands in your script you need to add an `enable` (Privileged Exec mode) command to the start of your script. If you need to run Global Configuration commands in your script you need to add a `configure terminal` command after the `enable` command at the start of your script.

The `activate` command executes the script in a new shell. A `terminal length` shell command, such as `terminal length 0` may also be required to disable a delay that would pause the display.

A script must be a text file with a filename extension of either `.sh` or `.scp` only for the AlliedWare Plus™ CLI to activate the script file. The `.sh` filename extension indicates the file is an ASH script, and the `.scp` filename extension indicates the file is an AlliedWare Plus™ script.

**Examples**
To activate a command script to run as a background process, use the command:

```
awplus# activate background test.scp
```

**Related Commands**
- `configure terminal`
- `echo`
- `enable` (Privileged Exec mode)
- `wait`
**echo**

**Overview**  
This command echoes a string to the terminal, followed by a blank line.

**Syntax**  
`echo <line>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;line&gt;</code></td>
<td>The string to echo</td>
</tr>
</tbody>
</table>

**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>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;delay&gt;</td>
<td>&lt;1-65335&gt; Specify the time delay in seconds</td>
</tr>
</tbody>
</table>

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

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

**Usage**  
Use this command to pause script execution in an .scp (AlliedWare Plus™ script) or an .sh (ASH script) file executed by the activate command. The script must contain an enable (Privileged Exec mode) command since the wait command is only executed in the Privileged Exec mode. When a script is activated, the privilege level is set to 1 enabling User Exec commands to run in the script. If you need to run Privileged Exec commands in your script you need to add an enable (Privileged Exec mode) command to the start of your script.

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

```plaintext
enable
show interface port1.0.1
wait 10
show interface port1.0.1
```

**Related Commands**  
activate  
echo  
enable (Privileged Exec mode)
Introduction

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

Command List  •  “description (interface)” on page 356
  •  “interface (to configure)” on page 357
  •  “mru” on page 359
  •  “mtu” on page 361
  •  “show interface” on page 363
  •  “show interface brief” on page 368
  •  “show interface status” on page 369
  •  “shutdown” on page 372
description (interface)

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

**Syntax**  
description <description>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;description&gt;</td>
<td>Text describing the specific interface.</td>
</tr>
</tbody>
</table>

**Mode**  Interface Configuration

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

```plaintext
awplus# configure terminal
awplus(config-if)# description Boardroom PC
```
interface (to configure)

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

Syntax
interface <interface-list>

interface lo

Usage
A local loopback interface is one that is always available for higher layer protocols to use and advertise to the network. Although a local loopback interface is assigned an IP address, it does not have the usual requirement of connecting to a lower layer physical entity. This lack of physical attachment creates the perception of a local loopback interface always being accessible via the network.

Local loopback interfaces can be utilized by a number of protocols for various purposes. They can be used to improve access to the device and also increase its reliability, security, scalability and protection. In addition, local loopback interfaces can add flexibility and simplify management, information gathering and filtering.

One example of this increased reliability is for OSPF to advertise a local loopback interface as an interface-route into the network irrespective of the physical links that may be “up” or “down” at the time. This provides a higher probability that the routing traffic will be received and subsequently forwarded.

Mode
Global Configuration

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

awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)#
The following example shows how to enter Interface mode to configure the local loopback interface.

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)#
```

**Related Commands**
- `ip address`
- `show interface`
- `show interface brief`
 INTERFACE COMMANDS

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

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

These additional components increase the frame size internally to 1522 bytes.

Syntax
mru <mru-size>
no mru

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mru-size&gt;</td>
<td>&lt;68-16357&gt; Specifies the Maximum Receive Unit (MRU) size in bytes, where 1500 bytes is the default Ethernet MRU size for an interface.</td>
</tr>
</tbody>
</table>

Default
The default MRU size is 1500 bytes for switch ports.

Mode
Interface Configuration for switch ports.

Usage
Note that show interface output will only show MRU size for switch ports.

Examples
To configure an MRU of 16357 bytes on port1.0.2, use the commands:

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# mru 16357

To configure an MRU of 1500 bytes on port1.0.2 to port1.0.4 use the commands:

awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# mru 1500
To restore the MRU size of 1500 bytes on port1.0.2, use the commands:

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

**Related Commands**
show interface
### mtu

**Overview**
Use this command to set the Maximum Transmission Unit (MTU) size for VLANs, where MTU is the maximum packet size that VLANs can transmit. The MTU size setting is applied to both IPv4 and IPv6 packet transmission.

Use the no variant of this command to remove a previously specified Maximum Transmission Unit (MTU) size for VLANs, and restore the default MTU size (1500 bytes) for VLANs.

**Syntax**

```
mtu <mtu-size>
no mtu
```

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

**Mode**
Interface Configuration for VLAN interfaces.

**Usage**
If a device receives an IPv4 packet for Layer 3 switching to another VLAN with an MTU size smaller than the packet size, and if the packet has the ‘don’t fragment’ bit set, then the device will send an ICMP ‘destination unreachable’ (3) packet type and a ‘fragmentation needed and DF set’ (4) code back to the source. For IPv6 packets bigger than the MTU size of the transmitting VLAN interface, an ICMP ‘packet too big’ (ICMP type 2 code 0) message is sent to the source.

Note that show interface output will only show MTU size for VLAN interfaces.

**Examples**
To configure an MTU size of 1500 bytes on interface vlan2, use the commands:

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

To configure an MTU size of 1500 bytes on interfaces vlan2 to vlan4, use the commands:

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

To restore the MTU size to the default MTU size of 1500 bytes on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no mtu
```
To restore the MTU size to the default MTU size of 1500 bytes on vlan2 and vlan4, use the commands

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

**Related Commands**

`show interface`
show interface

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

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
show interface [interface-list]

```
show interface lo
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-list&gt;</td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>- an interface such as a VLAN (e.g. vlan2), a switch port (e.g. port1.0.6),</td>
</tr>
<tr>
<td></td>
<td>a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g.</td>
</tr>
<tr>
<td></td>
<td>po2)</td>
</tr>
<tr>
<td></td>
<td>- a continuous range of interfaces, ports, static channel groups or dynamic</td>
</tr>
<tr>
<td></td>
<td>(LACP) channel groups separated by a hyphen; e.g. vlan2-8, or port1.0.1-1.0.6,</td>
</tr>
<tr>
<td></td>
<td>or sa1-2, or po1-2</td>
</tr>
<tr>
<td></td>
<td>- a comma-separated list of the above; e.g.</td>
</tr>
<tr>
<td></td>
<td>port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</td>
</tr>
</tbody>
</table>

The specified interfaces must exist.

| lo            | The local loopback interface.                                              |

**Mode**
User Exec and Privileged Exec

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

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

```
awplus# show interface
```
Figure 8-1: Example output from the `show interface` command
awplus#show interface

**Interface port1.0.1**
Scope: both
Link is UP, administrative state is UP
Thrash-limiting
Status Not Detected, Action link-down, Timeout 60(s)
Hardware is Ethernet, address is 0000.cd24.daeb
index 5001 metric 1 mru 1500
<UP,BROADCAST,RUNNING,MULTICAST>
current duplex half, current speed 100
configured duplex auto, configured speed auto, configured polarity auto
configured ecofriendly lpi
SNMP link-status traps: Sending (Suppressed after 20 traps in 60 sec.)
input packets 2396, bytes 324820, dropped 0, multicast packets 2370
output packets 73235, bytes 406566, multicast packets 7321 broadcast packets 7
Time since last state change: 0 days 16:35:52

**Interface port2.0.2**
Scope: both
Link is DOWN, administrative state is UP
Thrash-limiting
Status Unknown, Action learn-disable, Timeout 1(s)
Hardware is Provisioned, address is 0000.0000.0000
index 8001 metric 1 mru 1500
<BROADCAST,MULTICAST>
current duplex half, current speed 100
configured duplex auto, configured speed auto, configured polarity auto
configured ecofriendly lpi
configured ecofriendly lpi
SNMP link-status traps: Disabled
input packets 0, bytes 0, dropped 0, multicast packets 0
output packets 0, bytes 0, multicast packets 0 broadcast packets 0
Time since last state change: 0 days 16:35:52

**Interface lo**
Scope: both
Link is UP, administrative state is UP
Hardware is Loopback
index 1 metric 1
<UP,LOOPBACK,RUNNING>
SNMP link-status traps: Disabled
input packets 0, bytes 0, dropped 0, multicast packets 0
output packets 0, bytes 0, multicast packets 0 broadcast packets 0
Time since last state change: 0 days 16:35:52

**Interface vlan1**
Scope: both
Link is DOWN, administrative state is UP
Hardware is VLAN, address is 0000.cd24.daa8
index 201 metric 1 mtu 1500
arp ageing timeout 300
<VRF Binding: Not bound>
SNMP link-status traps: Disabled
Bandwidth 1g
input packets 0, bytes 0, dropped 0, multicast packets 0
output packets 29, bytes 1334, multicast packets 0 broadcast packets 0
Time since last state change: 0 days 05:36:40
To display configuration and status information for interface `lo`, use the command:

```
awplus# show interface lo
```

Figure 8-2: Example output from the `show interface lo` command

```
awplus# show interface lo
Interface lo
 Scope: both
 Link is UP, administrative state is UP
 Hardware is Loopback
 index 1 metric 1
 <UP,LOOPBACK,RUNNING>
 SNMP link-status traps: Disabled
   input packets 0, bytes 0, dropped 0, multicast packets 0
   output packets 0, bytes 0, multicast packets 0 broadcast packets 0
 Time since last state change: 69 days 01:28:47
```

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

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

Figure 8-3: Example output from the `show interface vlan1,vlan2` command

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

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

**Overview**  
Use this command to display brief interface, configuration, and status information, including provisioning information.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show interface brief

**Mode**  
User Exec and Privileged Exec

**Output**  
Figure 8-4: Example output from the `show interface brief` command

```
awplus#show int 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 8-1: Parameters in the output of the `show interface brief` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The name or type of interface.</td>
</tr>
<tr>
<td>Status</td>
<td>The administrative state. This can be either <code>admin up</code> or <code>admin down</code>.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The link state. This can be either <code>down</code>, <code>running</code>, or <code>provisioned</code>.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show interface`
- `show interface memory`
show interface status

**Overview**  Use this command to display the status of the specified interface or interfaces. Note that when no interface or interfaces are specified then the status of all interfaces on the device are shown.

**Syntax**  show interface [<port-list>] status

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports to display information about. The port list can be:</td>
</tr>
<tr>
<td></td>
<td>• a switch port (e.g. port1.0.6) or a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.6, or sa1-2, or po1-2</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
</tbody>
</table>

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

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

Table 8-2:  Example output from the `show interface <port-list> status` command

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Status</th>
<th>Vlan</th>
<th>Duplex</th>
<th>Speed</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.1</td>
<td></td>
<td>notconnect</td>
<td>1</td>
<td>auto</td>
<td>auto</td>
<td>1000BASE-T</td>
</tr>
<tr>
<td>port1.0.2</td>
<td></td>
<td>notconnect</td>
<td>1</td>
<td>auto</td>
<td>auto</td>
<td>1000BASE-T</td>
</tr>
<tr>
<td>port1.0.3</td>
<td></td>
<td>notconnect</td>
<td>1</td>
<td>auto</td>
<td>auto</td>
<td>1000BASE-T</td>
</tr>
<tr>
<td>port1.0.4</td>
<td></td>
<td>notconnect</td>
<td>1</td>
<td>auto</td>
<td>auto</td>
<td>1000BASE-T</td>
</tr>
</tbody>
</table>

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

```bash
awplus# show interface status
```


Table 8-3: Example output from the `show interface status` command

```
awplus#sho int 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             5 full       100 1000BaseTX
port1.0.3 Access_Net1        disabled              5 auto       auto 1000BaseTX
port1.0.4 Access_Net2        connected             6 a-half   a-100 1000BaseTX
port1.0.5 Private_Prom       connected            10 a-full   a-100 1000BaseTX
port1.0.6 Private_Net1       connected         10,11 a-full   a-100 1000BaseTX
port1.0.7 Private_Net2       connected         10,12 a-full   a-100 1000BaseTX
port1.0.8                    notconnect            1 auto      auto 1000BaseTX
port1.0.23                  disabled              1 auto      auto not present
port1.0.24                  notconnect        trunk auto      auto unknown
sa1                          notconnect        trunk auto      auto unknown
```

Table 8-4: Parameters in the output from the `show interface status` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Name/Type of the interface.</td>
</tr>
<tr>
<td>Name</td>
<td>Description of the interface.</td>
</tr>
</tbody>
</table>
| 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 port is an Eth port, it displays **none**: there is no VLAN associated with it.  
|           | • 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. |
### Table 8-4: Parameters in the output from the `show interface status` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>The actual link speed of the interface, preceded by <code>a-</code> if it has autonegotiated this speed. If the port is disabled or not connected, it displays the configured speed setting.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of interface, e.g. 1000BaseTX. For SFP bays, it displays <strong>Unknown</strong> if it does not recognize the type of SFP installed, or <strong>Not present</strong> if an SFP is not installed or is faulty.</td>
</tr>
</tbody>
</table>

**Related Commands**
- `show interface`
- `show interface memory`
shutdown

Overview  
This command shuts down the selected interface. This administratively disables the link and takes the link down at the physical (electrical) layer. 
Use the no variant of this command to disable this function and therefore to bring the link back up again.

Syntax  
shutdown 
no shutdown

Mode  
Interface Configuration

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

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

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

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

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

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

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

awplus# configure terminal  
awplus(config)# interface vlan2  
awplus(config-if)# no shutdown
9 Interface Testing Commands

Introduction

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

Command List

- “clear test interface” on page 374
- “service test” on page 375
- “test interface” on page 376
clear test interface

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports to test. A port-list can be:</td>
</tr>
<tr>
<td></td>
<td>• a switch port (e.g. port1.0.6)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of ports separated by a hyphen, e.g. port1.0.1-port1.0.6</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above, e.g. port1.0.1, port1.0.5-1.0.6</td>
</tr>
<tr>
<td>all</td>
<td>All interfaces</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

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

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

To clear the counters for all interfaces use the command:

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

**Related Commands**  test interface
service test

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

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

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

**Syntax**  

```
service test
no service test
```

**Mode**  Global Configuration

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

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

**Related Commands**  `test interface`
test interface

**Overview**  This command starts a test on a port or all ports or a selected range or list of ports. Use the `no` variant of this command to disable this function. The test duration can be configured by specifying the time in minutes after specifying a port or ports to test.

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `<port-list>` | The ports to test. A 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-port1.0.6`  
  - a comma-separated list of the above, e.g. `port1.0.1,port1.0.5-1.0.6`  
  The specified ports must exist. |
| `all` | All ports |
| `time` | Keyword entered prior to the value for the time duration of the interface test. |
| `<1-60>` | Specifies duration of time to test the interface or interfaces in minutes (from a minimum of 1 minute to a maximum of 60 minutes). The default is 4 minutes. |
| `cont` | Specifies continuous interface testing until canceled with command negation. |

**Mode**  Privileged Exec

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

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

TEST INTERFACE

To see the output, use the commands:

```
awplus# show test
awplus# show test count
```

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

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

Related Commands

```
clear test interface
```
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 381
- “clear loop-protection counters” on page 383
- “clear mac address-table static” on page 384
- “clear mac address-table dynamic” on page 385
- “clear port counter” on page 387
- “debug loopprot” on page 388
- “debug platform packet” on page 389
- “duplex” on page 391
- “flowcontrol (switch port)” on page 392
- “linkflap action” on page 394
- “loop-protection” on page 395
- “loop-protection action” on page 397
- “loop-protection action-delay-time” on page 398
- “loop-protection timeout” on page 399
- “mac address-table acquire” on page 400
- “mac address-table ageing-time” on page 401
- “mac address-table static” on page 402
- “mac address-table thrash-limit” on page 403
- “mirror interface” on page 404
- “platform hwfilter-size” on page 406
- “platform load-balancing” on page 407
- “platform stop-unreg-mc-flooding” on page 408
- “platform vlan-stacking-tpid” on page 410
- “polarity” on page 411
- “show debugging loopprot” on page 412
- “show debugging platform packet” on page 413
- “show flowcontrol interface” on page 414
- “show interface err-disabled” on page 415
- “show interface switchport” on page 416
- “show loop-protection” on page 417
- “show mac address-table” on page 419
- “show mac address-table thrash-limit” on page 421
- “show mirror” on page 422
- “show mirror interface” on page 423
- “show platform” on page 424
SWITCHING COMMANDS

- “show platform classifier statistics utilization brief” on page 425
- “show platform port” on page 427
- “show port-security interface” on page 431
- “show port-security intrusion” on page 432
- “show storm-control” on page 433
- “speed” on page 435
- “storm-control level” on page 437
- “switchport port-security” on page 438
- “switchport port-security aging” on page 439
- “switchport port-security maximum” on page 440
- “switchport port-security violation” on page 441
- “thrash-limiting” on page 442
- “undebug loopprot” on page 444
- “undebug platform packet” on page 445
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**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>on</code></td>
<td>Enables half-duplex flow control.</td>
</tr>
<tr>
<td><code>off</code></td>
<td>Disables half-duplex flow control.</td>
</tr>
</tbody>
</table>

**Default**  Backpressure is turned off by default. You can determine whether an interface has backpressure enabled by viewing the running-config output; `backpressure on` is shown for interfaces if this feature is enabled.

**Mode**  Interface Configuration

**Usage**  The backpressure feature enables half duplex Ethernet ports to control traffic flow during congestion by preventing further packets arriving. Back pressure utilizes a pre-802.3x mechanism in order to apply Ethernet flow control to switch ports that are configured in the half duplex mode.

The flow control applied by the `flowcontrol (switch port)` command operates only on full-duplex links, whereas back pressure operates only on half-duplex links.

If a port has insufficient capacity to receive further frames, the device will simulate a collision by transmitting a 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 back pressure flow control on interfaces `port1.0.1-port1.0.2` enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# backpressure on
```
To disable back pressure flow control on interface port1.0.2 enter the following commands:

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

**Validation Commands**
- `show running-config`
- `show interface`

**Related Commands**
- `duplex`
clear loop-protection counters

**Overview**
Use this command to clear the counters for the Loop Protection counters.

**Syntax**
clear loop-protection [interface <port-list>] counters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>The interface whose counters are to be cleared.</td>
</tr>
<tr>
<td>&lt;port-list&gt;</td>
<td>A port, a port range, or an aggregated link.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Examples**
To clear the counter information for all interfaces:

```
awplus# clear loop-protection counters
```

To clear the counter information for a single port:

```
awplus# clear loop-protection interface port1.0.1 counters
```
clear mac address-table static

**Overview**
Use this command to clear the filtering database of all statically configured entries for a selected MAC address, interface, or VLAN.

**Syntax**
clear mac address-table static [address <mac-address>|interface <port>|vlan <vid>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Specify a MAC (Media Access Control) address to be cleared from the filtering database.</td>
</tr>
<tr>
<td>&lt;mac-address&gt;</td>
<td>Enter a MAC address to be cleared from the database in the format HHHH.HHHH.HHHH.</td>
</tr>
<tr>
<td>interface</td>
<td>Specify a switch port to be cleared from the filtering database.</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td>Specify the switch port from which address entries will be cleared. This can be a single switch port, (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2).</td>
</tr>
<tr>
<td>vlan</td>
<td>Specify a VLAN to be cleared from the filtering database.</td>
</tr>
<tr>
<td>&lt;vid&gt;</td>
<td>Enter a VID (VLAN ID) in the range 1-4094 to be cleared from the filtering database.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Usage**
Use this command with options to clear the filtering database of all entries made from the CLI for a given MAC address, interface or VLAN. Use this command without options to clear any entries made from the CLI.

Compare this usage with `clear mac address-table dynamic` command.

**Examples**
This example shows how to clear all filtering database entries configured through the CLI.

```
awplus# clear mac address-table static
```

This example shows how to clear all filtering database entries for a given interface configured through the CLI.

```
awplus# clear mac address-table static interface port1.0.3
```

This example shows how to clear filtering database entries filtering database entries configured through the CLI for a given mac address.

```
awplus# clear mac address-table static address 0202.0202.0202
```

**Related Commands**
clear mac address-table dynamic
mac address-table static
show mac address-table
clear mac address-table dynamic

**Overview**
Use this command to clear the filtering database of all entries learned for a selected MAC address, an MSTP instance, a switch port interface or a VLAN interface.

**Syntax**
clear mac address-table dynamic [address <mac-address>|interface <port> [instance <inst>]|vlan <vid>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specify a switch port to be cleared from the filtering database.</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td>Specify the switch port from which address entries will be cleared. This can be a single switch port, (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2).</td>
</tr>
<tr>
<td>address</td>
<td>Specify a MAC (Media Access Control) address to be cleared from the filtering database.</td>
</tr>
<tr>
<td>&lt;mac-address&gt;</td>
<td>Enter a MAC address to be cleared from the database in the format HHHH.HHHH.HHHH.</td>
</tr>
<tr>
<td>instance</td>
<td>Specify an MSTP (Multiple Spanning Tree) instance to be cleared from the filtering database.</td>
</tr>
<tr>
<td>&lt;inst&gt;</td>
<td>Enter an MSTP instance in the range &lt;1-63&gt; to be cleared from the filtering database.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specify a VLAN to be cleared from the filtering database.</td>
</tr>
<tr>
<td>&lt;vid&gt;</td>
<td>Enter a VID (VLAN ID) in the range &lt;1-4094&gt; to be cleared from the filtering database.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Usage**
Use this command with options to clear the filtering database of all entries learned for a given MAC address, interface or VLAN. Use this command without options to clear any learned entries.

Use the optional instance parameter to clear the filtering database entries associated with a specified MSTP instance. Note that you must first specify a switch port interface before you can specify an MSTP instance.

Compare this usage and operation with the clear mac address-table static command. Note that an MSTP instance cannot be specified with clear mac address-table static.

**Examples**
This example shows how to clear all dynamically learned filtering database entries for all interfaces, addresses, VLANs.

awplus# clear mac address-table dynamic
This example shows how to clear all dynamically learned filtering database entries when learned through device operation for a given MAC address.

```
awplus# clear mac address-table dynamic address 0202.0202.0202
```

This example shows how to clear all dynamically learned filtering database entries when learned through device operation for a given MSTP instance 1 on switch port interface port1.0.2.

```
awplus# clear mac address-table dynamic interface port1.0.2 instance 1
```

Related Commands

- clear mac address-table static
- show mac address-table
clear port counter

**Overview**  Use this command to clear the packet counters of the port.

**Syntax**  clear port counter [<port>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>The port number or range</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Example**  To clear the packet counter for port1.0.1, use the command:

    awplus# clear port counter port1.0.1

**Related Commands**  show platform port
**debug loopprot**

**Overview**  
This command enables Loop Protection debugging. The **no** variant of this command disables Loop Protection debugging.

**Syntax**  
debug loopprot {info|msg|pkt|state|nsm|all}  
no debug loopprot {info|msg|pkt|state|nsm|all}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>info</td>
<td>General Loop Protection information.</td>
</tr>
<tr>
<td>msg</td>
<td>Received and transmitted Loop Detection Frames (LDFs).</td>
</tr>
<tr>
<td>pkt</td>
<td>Echo raw ASCII display of received and transmitted LDF packets to the console.</td>
</tr>
<tr>
<td>state</td>
<td>Loop Protection states transitions.</td>
</tr>
<tr>
<td>nsm</td>
<td>Network Service Module information.</td>
</tr>
<tr>
<td>all</td>
<td>All debugging information.</td>
</tr>
</tbody>
</table>

**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 <vlan-id>|all]
no debug platform packet [recv] [send]
```

**Default**  
A 5 minute timeout is configured by default if no other timeout duration is specified.

**Mode**  
Privileged Exec and Global Configuration

**Usage**  
This command can be used to trace packets sent and received by the CPU. If a timeout is not specified, then a default 5 minute timeout will be applied.

If a timeout of 0 is specified, packet debug will be generated until the `no` variant of this command is used or another timeout value is specified. The timeout value applies to both send and receive debug and is updated whenever the `debug platform packet` command is used.

**Examples**  
To enable both receive and send packet debug for the default timeout of 5 minutes, enter:

```
awplus# debug platform packet
```

To enable receive packet debug for 10 seconds, enter:

```
awplus# debug platform packet recv timeout 10
```
To enable 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 2 with a timeout duration of 3 minutes, enter:

```
awplus# debug platform packet vlan 2 timeout 150
```

To disable receive packet debug, enter:

```
awplus# no debug platform packet recv
```

**Related Commands**

- `show debugging platform packet`
- `undebug platform packet`
**duplex**

**Overview**
This command changes the duplex mode for the specified port.

To see the currently-negotiated duplex mode for ports whose links are up, use the command `show interface`. To see the configured duplex mode (when different from the default), use the command `show running-config`.

**Syntax**
duplex {auto|full|half}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Auto-negotiate duplex mode.</td>
</tr>
<tr>
<td>full</td>
<td>Operate in full duplex mode only.</td>
</tr>
<tr>
<td>half</td>
<td>Operate in half duplex mode only.</td>
</tr>
</tbody>
</table>

**Default**
By default, ports auto-negotiate duplex mode (except for 100Base-FX ports which do not support auto-negotiation, so default to full duplex mode).

**Mode**
Interface Configuration

**Usage**
switch ports in a static or dynamic (LACP) channel group must have the same port speed and be in full duplex mode. Once switch ports have been aggregated into a channel group, you can set the duplex mode of all the switch ports in the channel group by applying this command to the channel group.

**Examples**
To specify full duplex for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex full
```

To specify half duplex for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex half
```

To auto-negotiate duplex mode for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex auto
```

**Related Commands**
backpressure
polarity
speed
show interface
flowcontrol (switch port)

**Overview**
Use this command to enable flow control, and configure the flow control mode for the switch port.

Use the `no` variant of this command to disable flow control for the specified switch port.

**Syntax**
```
flowcontrol {send|receive} {off|on}
no flowcontrol
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>receive</td>
<td>When the port receives pause frames, it temporarily stops (pauses) sending traffic.</td>
</tr>
<tr>
<td>on</td>
<td>Enable the specified flow control.</td>
</tr>
<tr>
<td>off</td>
<td>Disable the specified flow control.</td>
</tr>
<tr>
<td>send</td>
<td>When the port is congested (receiving too much traffic), it sends pause frames to request the other end to temporarily stop (pause) sending traffic.</td>
</tr>
</tbody>
</table>

**Default**
By default, flow control is disabled.

**Mode**
Interface Configuration

**Usage**
The flow control mechanism specified by 802.3x is only for full duplex links. It operates by sending PAUSE frames to the link partner to temporarily suspend transmission on the link.

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion, and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When the local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the congestion period.

Flow control is not recommended when running QoS or ACLs, because the complex queuing, scheduling, and filtering configured by QoS or ACLs may be slowed by applying flow control.

For half-duplex links, an older form of flow control known as backpressure is supported. See the related `backpressure` command.

For flow control on async serial (console) ports, see the `flowcontrol hardware (asyn/console)` command.
Examples

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol receive on
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol send on
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol receive off
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol send off

Validation Commands

show running-config

Related Commands

backpressure
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linkflap</td>
<td>Global setting for link flapping.</td>
</tr>
<tr>
<td>action</td>
<td>Specify the action for port.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shutdown the port.</td>
</tr>
</tbody>
</table>

Default  Linkflap action is disabled by default.

Mode  Global Configuration

Example  To enable the linkflap action command on the device, use the following commands:

awplus# configure terminal
awplus(config)# linkflap action shutdown
# loop-protection

## Overview

Use this command to enable the loop-protection loop-detection feature, and configure the detection mechanism parameters.

Use the `no` variant of this command to disable the loop-protection loop-detection feature.

## Syntax

```
loop-protection loop-detect [ldf-interval <period>]
[ldf-rx-window <frames>] [fast-block]
no loop-protection [loop-detect]
```

## Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>loop-detect</code></td>
<td>Enables loop detection when used with loop-protection keywords. Disables loop detection when used with no loop-protection keywords.</td>
</tr>
<tr>
<td><code>ldf-interval</code></td>
<td>The time (in seconds) between successive loop-detect frames being sent.</td>
</tr>
<tr>
<td><code>&lt;period&gt;</code></td>
<td>Specify a period between 1 and 600 seconds. The default is 10 seconds.</td>
</tr>
<tr>
<td><code>ldf-rx-window</code></td>
<td>The number of transmitted loop detection frames whose details are held for comparing with frames arriving at the same port.</td>
</tr>
<tr>
<td><code>&lt;frames&gt;</code></td>
<td>Specify a value for the window size between 1 and 5 frames. The default is 3 frames.</td>
</tr>
<tr>
<td><code>[fast-block]</code></td>
<td>The fast-block blocks transmitting port to keep partial connectivity.</td>
</tr>
</tbody>
</table>

## Default

The loop-protection loop-detection feature is disabled by default. The default interval is 10 seconds, and the default window size is 3 frames.

## Mode

Global Configuration

## Usage

See the “Loop Protection” section in the Switching Feature Overview and Configuration Guide for relevant conceptual, configuration, and overview information prior to applying this command.

## Example

To enable the loop-detect mechanism on the switch, and generate loop-detect frames once every 5 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# loop-protection loop-detect ldf-interval 5
```
<table>
<thead>
<tr>
<th><strong>Related Commands</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>loop-protection action</td>
</tr>
<tr>
<td>loop-protection timeout</td>
</tr>
<tr>
<td>show loop-protection</td>
</tr>
<tr>
<td>thrash-limiting</td>
</tr>
</tbody>
</table>
**loop-protection action**

**Overview**
Use this command to specify the protective action to apply when a network loop is detected on an interface.

Use the `no` variant of this command to reset the loop protection actions to the default action, vlan-disable, on an interface.

**NOTE:** Currently the learn-disable parameter is not supported. If specified, an error message will be displayed.

**Syntax**

```
loop-protection
action {link-down|log-only|port-disable|vlan-disable|none}
no loop-protection action
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-down</td>
<td>Block all traffic on a port (or aggregated link) that detected the loop, and take <strong>down</strong> the link.</td>
</tr>
<tr>
<td>log-only</td>
<td>Details of loop conditions are logged. No action is applied to the port (or aggregated link).</td>
</tr>
<tr>
<td>port-disable</td>
<td>Block all traffic on interface for which the loop occurred, but keep the link in the <strong>up</strong> state.</td>
</tr>
<tr>
<td>vlan-disable</td>
<td>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.</td>
</tr>
<tr>
<td>none</td>
<td>Applies no protective action.</td>
</tr>
</tbody>
</table>

**Default**
loop-protection action vlan-disable

**Mode**
Interface Configuration

**Usage**
See the “Loop Protection” section in the Switching Feature Overview and Configuration Guide for relevant conceptual, configuration, and overview information prior to applying this command.

**Example**
To disable an interface (`port1.0.4`), and bring the link down, when a network loop is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection action link-down
```

**Related Commands**
- loop-protection
- loop-protection timeout
- show loop-protection
- thrash-limiting
**loop-protection action-delay-time**

**Overview**  
Use this command to set 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>
noloop-protection action
```

**Default**  
Action delay timer is disabled by default.

**Mode**  
Interface Configuration

**Example**  
To configure a loop protection action delay time of 10 seconds, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection action-delay-time 10
```

To reset the Loop Protection action delay time to default, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.1.4
awplus(config-if)# no loop-protection action-delay-time
```

**Related Commands**  
`show loop-protection`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;0-86400&gt;</code></td>
<td>Time in seconds; 0 means action delay timer is disabled.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;duration&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Default**  
The default is 7 seconds.

**Mode**  
Interface Configuration

**Usage**  
See the “Loop Protection” section in the Switching Feature Overview and Configuration Guide for relevant conceptual, configuration, and overview information prior to applying this command.

**Example**  
To configure a loop protection action timeout of 10 seconds for port1.0.4, use the command:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection timeout 10
```

**Related Commands**  
loop-protection  
loop-protection action  
show loop-protection  
thrash-limiting
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ageing-timer&gt;</td>
<td>&lt;10-1000000&gt; The number of seconds of persistence.</td>
</tr>
<tr>
<td>none</td>
<td>Disable learned MAC address timeout.</td>
</tr>
</tbody>
</table>

**Default**  The default ageing time is 300 seconds.

**Mode**  Global Configuration

**Examples**  The following commands specify various ageing timeouts on the device:

```
awplus# configure terminal
awplus(config)# mac address-table ageing-time 1000
awplus# configure terminal
awplus(config)# mac address-table ageing-time none
awplus# configure terminal
awplus(config)# no mac address-table ageing-time
```
mac address-table static

**Overview**  
Use this command to statically configure the MAC address-table to forward or discard frames with a matching destination MAC address.

**Syntax**  
mac address-table static <mac-addr> {forward|discard} interface <port> [vlan <vid>]
no mac address-table static <mac-addr> {forward|discard} interface <port> [vlan <vid>]

**Parameter** | **Description**
--- | ---
<mac-addr> | The destination MAC address in HHHH.HHHH.HHHH format.
<port> | The port to display information about. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2).
<vid> | The VLAN ID. If you do not specify a VLAN, its value defaults to vlan 1.

**Mode**  
Global Configuration

**Usage**  
The **mac address-table static** command is only applicable to Layer 2 switched traffic within a single VLAN. Do not apply the **mac address-table static** command to Layer 3 switched traffic passing from one VLAN to another VLAN. Frames will not be discarded across VLANs because packets are routed across VLANs. This command only works on Layer 2 traffic.

**Example**  
awplus# configure terminal
awplus(config)# mac address-table static 2222.2222.2222 forward
interface port1.0.4 vlan 3

**Related Commands**
clear mac address-table static
show mac address-table
mac address-table thrash-limit

**Overview**
Use this command to set the thrash limit on the device or stack.

Thrashing occurs when a MAC address table rapidly “flips” its mapping of a single MAC address between two subnets, usually as a result of a network loop.

Use the no variant of this command to disable thrash limiting.

**Syntax**

mac address-table thrash-limit <rate>

no mac address-table thrash-limit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;rate&gt;</td>
<td>sets the maximum thrash rate at which limiting is applied. This rate can be set between 5 and 255 MAC thrashing flips per second. Once the thrash limit rate is reached, the port is considered to be thrashing.</td>
</tr>
</tbody>
</table>

**Default**
No thrash limiting

**Mode**
Global Configuration

**Usage**
Use this command to limit thrashing on the selected port range.

**Example**
To apply a thrash limit of 100 MAC address flips per second:

```
awplus# configure terminal
awplus(config)# mac address-table thrash-limit 100
```

**Related Commands**
show mac address-table thrash-limit
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;source-port-list&gt;</td>
<td>The source switch ports to mirror. A port-list can be:</td>
</tr>
<tr>
<td></td>
<td>• a port (e.g. port1.0.2)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of ports separated by a hyphen, e.g.</td>
</tr>
<tr>
<td></td>
<td>port1.0.1-1.0.2</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of ports and port ranges, e.g.</td>
</tr>
<tr>
<td></td>
<td>port1.0.1,port1.0.4-1.0.6</td>
</tr>
<tr>
<td>direction</td>
<td>Specifies whether to mirror traffic that the source port</td>
</tr>
<tr>
<td></td>
<td>receives, transmits, or both.</td>
</tr>
<tr>
<td>both</td>
<td>Mirroring traffic both received and transmitted by the source port.</td>
</tr>
<tr>
<td>receive</td>
<td>Mirroring traffic received by the source port.</td>
</tr>
<tr>
<td>transmit</td>
<td>Mirroring traffic transmitted by the source port.</td>
</tr>
<tr>
<td>none</td>
<td>Specify this parameter for use with the ACL (Access Control List) access-list and QoS (Quality of Service) default action commands when used with the copy-to-mirror parameter option, so you can specify the destination port (the analyzer port) for the traffic without specifying a source mirror port. See the ACL commands access-list (hardware IP numbered) and access-list (hardware MAC numbered), and the QoS command default-action for further information.</td>
</tr>
</tbody>
</table>

Mode
Interface Configuration
**Usage**  
Use this command to send traffic to another device connected to the mirror port for monitoring.

See the “Port Mirroring” section in the Switching Feature Overview and Configuration Guide for more information.

A mirror port cannot be associated with a VLAN. If a switch port is configured to be a mirror port, it is automatically removed from any VLAN it was associated with.

This command can only be applied to a single mirror (destination) port, not to a range of ports, nor to a static or dynamic channel group. Do not apply multiple interfaces with an interface command before issuing the mirror interface command. One interface may have multiple mirror interfaces.

**Example**  
To mirror traffic received and transmitted on port1.0.4 and port1.0.5 to destination port1.0.3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# mirror interface port1.0.4,port1.0.5 direction both
```

To enable use with the access-list (hardware IP numbered) ACL and default-action QoS commands to destination port1.0.3 without specifying a source port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# mirror interface none
```

To mirror all TCP traffic, received or transmitted to analyzer port1.0.1, see the sample config 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
  switchport
!
```

**Related Commands**
- access-list (hardware IP numbered)
- access-list (hardware MAC numbered)
- default-action
**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.

One 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}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hwfilter-size</td>
<td>Configure hardware ACLs command.</td>
</tr>
<tr>
<td>ipv4-full-ipv6</td>
<td>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.</td>
</tr>
<tr>
<td>ipv4-limited-ipv6</td>
<td>Configure hardware ACLs to filter IPv4 traffic, MAC addresses and IPv6 traffic. Source or destination IPv6 addresses or both are not filtered.</td>
</tr>
</tbody>
</table>

**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)`
# 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
```

## Default
The default is **src-dst-ip**.

## Mode
Global configuration

## Examples
To set the load balancing algorithm to include only Layer 2 MAC addresses, enter:
```
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 L4 ports, enter:
```
awplus# configure terminal
awplus(config)# platform load-balancing src-dst-ip
```

## Related Commands
- `show platform`
platform stop-unreg-mc-flooding

**Overview**  
This command stops multicast packets flooding out of all the ports in the VLAN until these packets are registered. This command does this by sending unregistered multicast packets to the switch processor, so there is no flooding of the multicast traffic onto the VLAN. Unregistered traffic will not flow until the switch has registered it, regardless of attempts to subscribe to it. Once the traffic is registered, it flows to registered subscribers and ports.

Use the **no** variant of this command to revert to default behavior and disable this feature.

*NOTE:* This command should not be used within any IPv6 networks.

IPv6 neighbor discovery operation is inhibited by this feature.

This command does not stop reserved Local Network Control Block IPv4 multicast packets in the address range 224.0.0.1 to 224.0.0.255 (224.0.0/24).

See [www.iana.org/assignments/multicast-addresses/multicast-addresses.xml#multicast-addresses-1](http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml#multicast-addresses-1)

**Syntax**

```
platform stop-unreg-mc-flooding
no platform stop-unreg-mc-flooding
```

**Default**  
This feature is disabled by default.

**Mode**  
Global Configuration

**Usage**  
This command stops the periodic flooding of unknown or unregistered multicast packets when the Group Membership interval timer expires and there are no subscribers to a multicast group. If there is multicast traffic in a VLAN without subscribers, multicast traffic temporarily floods out of the VLAN when the Group Membership interval timer expires, which happens when the switch does not get replies from Group Membership queries.

This command also stops the initial flood of multicast packets that happens when a new multicast source starts to send traffic. This flooding lasts until snooping recognizes the multicast group. For example, in sites where IP cameras have multicast groups, traffic is flooded to the VLAN and causes large bursts of traffic. Use this command when there is limited processing available for large bursts of traffic, such as in sites with IP cameras.

**Output**  
See the console message warning about IPv6 operation after entering this command:

```
% WARNING: IPv6 will not work with this setting enabled
% Please consult the documentation for more information
```
See these sample console messages when the Group Membership interval timer expires, which happens when the switch does not get replies from Group Membership queries:

```
awplus: [MLD-EVENTS] Grp - Rec Liveness Timer: Expiry for Grp ff0e::1 on port1.2.7
awplus: [IGMP-EVENTS]: Expiry (Unreg MC Timer) for Grp 224.2.2.2 on vlan4
```

**Examples**

To enable this feature and stop multicast packet flooding, use the following commands:

```
awplus# configure terminal
awplus(config)# platform stop-unreg-mc-flooding
```

To disable this feature and allow multicast packet flooding, use the following commands:

```
awplus# configure terminal
awplus(config)# no platform stop-unreg-mc-flooding
```

**Related Commands**

- `show platform`
- `show running-config`
platform vlan-stacking-tpid

**Overview**  This command specifies the Tag Protocol Identifier (TPID) value that applies to all frames that are carrying double tagged VLANs. All nested VLANs must use the same TPID value. (This feature is sometimes referred to as VLAN stacking or VLAN double-tagging.)

Use the **no** variant of this command to revert to the default TPID value (0x8100).

**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**  
```plaintext
platform vlan-stacking-tpid <tpid>
no platform vlan-stacking-tpid
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;tpid&gt;</td>
<td>The Ethernet type of the tagged packet, as a two byte hexadecimal number.</td>
</tr>
</tbody>
</table>

**Default**  The default TPID value is 0x8100.

**Mode**  Global Configuration

**Examples**  To set the VLAN stacking TPID value to 0x9100, use the following commands:

```plaintext
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:

```plaintext
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\}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdi</td>
<td>Sets the polarity to MDI (medium dependent interface).</td>
</tr>
<tr>
<td>mdix</td>
<td>Sets the polarity to MDI-X (medium dependent interface crossover).</td>
</tr>
<tr>
<td>auto</td>
<td>The switch port sets the polarity automatically. This is the default option.</td>
</tr>
</tbody>
</table>

**Default**
By default, switch ports set the polarity automatically (auto).

**Mode**
Interface Configuration

**Usage**
We recommend the default auto setting for MDI/MDIX polarity. Polarity applies to copper 10BASE-T, 100BASE-T, and 1000BASE-T switch ports; It does not apply to fiber ports. See the “MDI/MDIX Connection Modes” section in the Switching Feature Overview and Configuration Guide for more information.

**Example**
To set the polarity for port1.0.6 to fixed MDI mode, use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# polarity mdi
```
show debugging loopprot

**Overview**  This command shows Loop Protection debugging information.

**Syntax**  show debugging loopprot

**Mode**  User Exec and Privileged Exec

**Example**  To display the enabled Loop Protection debugging modes, use the command:

```
awplus# show debugging loopprot
```

**Related Commands**  debug loopprot
show debugging platform packet

**Overview**  This command shows platform to CPU level packet debugging information.

**Syntax**  show debugging platform packet

**Mode**  User Exec and Privileged Exec

**Example**  To display the platform packet debugging information, use the command:

```
awplus# show debugging platform packet
```

**Related Commands**
- debug platform packet
- undebug platform packet
show flowcontrol interface

**Overview**  Use this command to display flow control information.

**Syntax**  
```plaintext
show flowcontrol interface <port>
```

**Parameter**  | **Description**  
--- | ---  
[port] | Specifies the name of the port to be displayed.  

**Mode**  User Exec and Privileged Exec

**Example**  To display the flow control for the port1.0.5, use the command:

```plaintext
awplus# show flowcontrol interface port1.0.5
```

**Output**  Figure 10-1: Example output from the show flowcontrol interface command for a specific interface

<table>
<thead>
<tr>
<th>Port</th>
<th>Send FlowControl</th>
<th>Receive FlowControl</th>
<th>RxPause</th>
<th>TxPause</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.5</td>
<td>on</td>
<td>on</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
**show interface err-disabled**

**Overview**  Use this command to show the ports which have been dynamically shut down by protocols running on the device and the protocols responsible for the shutdown.

**Syntax**  
```
show interface [<IFRANGE> err-disabled]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IFRANGE&gt;</td>
<td>Interface range</td>
</tr>
<tr>
<td>err-disabled</td>
<td>Brief summary of interfaces shut down by protocols</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**  Show the protocols that have shut down port2.0.21 and port2.0.23, use the commands:

```
awplus# show interface err-disabled
```

**Output**  Figure 10-2: Example output from the **show interface err-disabled** command

```
awplus#show interface err-disabled
Interface   Reason
port2.0.21   loop protection
port2.0.23   loop protection
```
show interface switchport

Overview
Use this command to show VLAN information about each switch port.

Syntax
show interface switchport

Mode
User Exec and Privileged Exec

Example
To display VLAN information about each switch port, enter the command:

awplus# show interface switchport

Output
Figure 10-3: Example output from the show interface switchport command

<table>
<thead>
<tr>
<th>Interface name</th>
<th>Switchport mode</th>
<th>Ingress filter</th>
<th>Acceptable frame types</th>
<th>Default Vlan</th>
<th>Configured Vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.1</td>
<td>access</td>
<td>enable</td>
<td>all</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>port1.0.2</td>
<td>trunk</td>
<td>enable</td>
<td>all</td>
<td>1</td>
<td>1 4 5 6 7 8</td>
</tr>
</tbody>
</table>

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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>The interface selected for display.</td>
</tr>
<tr>
<td>&lt;port-list&gt;</td>
<td>A port, a port range, or an aggregated link.</td>
</tr>
<tr>
<td>counters</td>
<td>Displays counter information for loop protection.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Usage**
This command is used to display the current configuration and operation of the Loop Protection feature

**Examples**
To display the current configuration status for port1.0.1, use the command:
```
awplus# show loop-protection interface port1.0.1
```

Figure 10-4: Example output from the **show loop-protection** command

```
Loop-Detection:          Enabled
LDF Interval:            10 [sec]
Interface:               port1.0.1
Action:                  port-disable
Timeout:                 300 [sec]
Vlan:                    1
Status:                  Blocking
Timeout Remaining:       115 [sec]
Vlan:                    2
Status:                  Normal
Timeout Remaining:       0 [sec]
```

To display the counter information for port1.0.1, use the command:
```
awplus# show loop-protection interface port1.0.1 counters
```
Figure 10-5: Example output from the `show loop-protection interface counters` command for port 1.0.1

<table>
<thead>
<tr>
<th>Interface:</th>
<th>port1.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan:</td>
<td>1</td>
</tr>
<tr>
<td>LDF Tx:</td>
<td>3</td>
</tr>
<tr>
<td>LDF Rx:</td>
<td>1</td>
</tr>
<tr>
<td>Invalid LDF Rx:</td>
<td>1</td>
</tr>
<tr>
<td>Action:</td>
<td>1</td>
</tr>
<tr>
<td>Vlan:</td>
<td>2</td>
</tr>
<tr>
<td>LDF Tx:</td>
<td>3</td>
</tr>
<tr>
<td>LDF Rx:</td>
<td>0</td>
</tr>
<tr>
<td>Invalid LDF Rx:</td>
<td>0</td>
</tr>
<tr>
<td>Action:</td>
<td>0</td>
</tr>
</tbody>
</table>
show mac address-table

**Overview** Use this command to display the mac address-table for all configured VLANs.

**Syntax** show mac address-table

**Mode** User Exec and Privileged Exec

**Usage** The show mac address-table command is only applicable to view a mac address-table for Layer 2 switched traffic within VLANs.

**Example** To display the mac address-table, use the following command:

```
awplus# show mac address-table
```

**Output** See the below sample output captured when there was no traffic being switched:

```
awplus#show mac address-table
VLAN Port     MAC              State
1            unknown      0000.cd28.0752   static
ARP -         0000.cd00.0000   static
```

See the sample output captured when packets were switched and mac addresses were learned:

```
awplus#show mac address-table
VLAN Port     MAC              State
1            unknown      0000.cd28.0752   static
1            port1.0.6    0030.846e.9bf4   dynamic
1            port1.0.4    0030.846e.bac7   dynamic
ARP -         0000.cd00.0000   static
```

Note the new mac addresses learned for port1.0.4 and port1.0.6 added as dynamic entries.

Note the first column of the output below shows VLAN IDs if multiple VLANs are configured:

```
awplus#show mac address-table
VLAN Port     MAC              State
1            unknown      0000.cd28.0752   static
1            port1.0.6    0030.846e.9bf4   dynamic
2            unknown      0000.cd28.0752   static
2            port1.0.6    0030.846e.9bf4   dynamic
ARP -         0000.cd00.0000   static
```
Also note manually configured static mac-addresses are shown to the right of the type column:

```
awplus(config)#mac address-table static 0000.1111.2222 for int port1.0.3 vlan 2
awplus(config)#end
awplus#
awplus#show mac address-table

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Port</th>
<th>MAC</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>unknown</td>
<td>0000.cd28.0752</td>
<td>static</td>
</tr>
<tr>
<td>1</td>
<td>port1.0.2</td>
<td>0030.846e.bac7</td>
<td>dynamic</td>
</tr>
<tr>
<td>2</td>
<td>port1.0.3</td>
<td>0000.1111.2222</td>
<td>static</td>
</tr>
<tr>
<td>2</td>
<td>unknown</td>
<td>0000.cd28.0752</td>
<td>static</td>
</tr>
<tr>
<td>2</td>
<td>port1.0.5</td>
<td>0030.846e.9bf4</td>
<td>dynamic</td>
</tr>
<tr>
<td>ARP</td>
<td>-</td>
<td>0000.cd00.0000</td>
<td>statics</td>
</tr>
</tbody>
</table>
```

**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 10-6: 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 mirror

**Overview**
Use this command to display the status of all mirrored ports.

**Syntax**
show mirror

**Mode**
User Exec and Privileged Exec

**Example**
To display the status of all mirrored ports, use the following command:

```
awplus# show mirror
```

**Output**
Figure 10-7: Example output from the show mirror command

```
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.2
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.4
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.1
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.3
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: transmit
Monitored Port Name: port1.0.4
```
show mirror interface

**Overview**  Use this command to display port mirroring configuration for a mirrored (monitored) switch port.

**Syntax**  
```
show mirror interface <port>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>The monitored switch port to display information about.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec, Privileged Exec and Interface Configuration

**Example**  
To display port mirroring configuration for the `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# show mirror interface port1.0.4
```

**Output**  Figure 10-8: Example output from the `show mirror interface` command

```
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.4
```
show platform

**Overview**  This command displays the settings configured by using the `platform` commands.

**Syntax**  
```
show platform
```

**Mode**  Privileged Exec

**Usage**  This command displays the settings in the running config. For changes in some of these settings to take effect, the device must be rebooted with the new settings in the startup config.

**Example**  To check the settings configured with `platform` commands on the device, use the following command:

```
awplus# show platform
```

**Output**  

Figure 10-9:  Example output from the `show platform` command

```
awplus# show platform
Vlan-stacking TPID     0x8100
```

Table 10-1: Parameters in the output of the `show platform` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan-stacking TPID</td>
<td>The value of the TPID set in the Ethernet type field when a frame has a double VLAN tag (<code>platform vlan-stacking-tpid</code> command).</td>
</tr>
</tbody>
</table>

**Related Commands**

- `platform load-balancing`
- `platform vlan-stacking-tpid`
show platform classifier statistics utilization brief

**Overview**
This command displays the number of used entries available for various platform functions, and the percentage that number of entries represents of the total available.

**Syntax**
show platform classifier statistics utilization brief

**Mode**
Privileged Exec

**Example**
To display the platform classifier utilization statistics, use the following command:

```
awplus# show platform classifier statistics utilization brief
```

**Output**
Figure 10-10: Output from the `show platform classifier statistics utilization brief` command

```
[Instance 0]
Number of Entries:
Policy Type    Group ID    Used / Total
------------------------------------
ACL             1476395009  0 / 118 ( 0%)
Web Auth       Inactive    0 /  0 ( 0%)
QoS             0 /  128 ( 0%)
```

Figure 10-11: Output from the `show platform classifier statistics utilization brief` command

```
[Instance 3.0]
(Port1.0.1-1.0.24)
Number of Entries:
Policy Type    Group ID    Used / Total
------------------------------------
ACL             1476395009  0 / 122 ( 0%)
DoS             -1          0 /  0 ( 0%)
VLAN Counter    -1          0 /  0 ( 0%)
QoS             0 /  768 ( 0%)

[Instance 3.1]
(Port1.0.25-1.0.48)
Number of Entries:
Policy Type    Group ID    Used / Total
------------------------------------
ACL             1476395009  0 / 122 ( 0%)
DoS             -1          0 /  0 ( 0%)
VLAN Counter    -1          0 /  0 ( 0%)
QoS             2 /  768 ( 0%)
```
### Switching Commands

**SHOW PLATFORM CLASSIFIER STATISTICS UTILIZATION BRIEF**

Figure 10-12: Output from the `show platform classifier statistics utilization brief` command, with the DOS detection feature enabled

```
[Instance 3.0]
[Port1.0.1-1.0.24]
Number of Entries:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Group ID</th>
<th>Used / Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>1476395009</td>
<td>0 / 122 (0%)</td>
</tr>
<tr>
<td>DoS</td>
<td>1476395011</td>
<td>0 / 128 (0%)</td>
</tr>
<tr>
<td>VLAN Counter</td>
<td>-1</td>
<td>0 / 0 (0%)</td>
</tr>
<tr>
<td>QoS</td>
<td>0</td>
<td>640 (0%)</td>
</tr>
</tbody>
</table>

[Instance 3.1]
[Port1.0.25-1.0.48]
Number of Entries:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Group ID</th>
<th>Used / Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>1476395009</td>
<td>0 / 122 (0%)</td>
</tr>
<tr>
<td>DoS</td>
<td>1476395011</td>
<td>1 / 128 (0%)</td>
</tr>
<tr>
<td>VLAN Counter</td>
<td>-1</td>
<td>0 / 0 (0%)</td>
</tr>
<tr>
<td>QoS</td>
<td>2</td>
<td>640 (0%)</td>
</tr>
</tbody>
</table>

1 2 / 128 (1%)
```

---

**Related Commands**

- `show platform`
show platform port

**Overview**  This command displays the various port registers or platform counters for specified switchports.

**Syntax**  show platform port [<port-list>|counters]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| <port-list> | The ports to display information about. A port-list can be:  
|             | - 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,port1.0.4-1.0.6.  |
| counters    | Show the platform counters.  |

**Mode**  Privileged Exec

**Examples**  To display port registers for port1.0.1 and port1.0.2 use the following command:  
awplus# show platform port port1.0.1-port1.0.2

To display platform counters for port1.0.1 and port1.0.2 use the following command:  
awplus# show platform port port1.0.1-port1.0.2 counters
Output

Figure 10-13: Example output from the `show platform port` command

```
awplus#show platform port port1.0.1
Phy register value for port1.0.1 (ifindex: 5001)
00:1140  01:7949  02:0020  03:60B1  04:01E1  05:0000  06:0004  07:2001
08:0000  09:0600  10:0000  11:0000  12:0000  13:0000  14:0000  15:0000
16:0000  17:0000  18:0000  19:0000  20:0000  21:0000  22:0000  23:0000
24:0000  25:0000  26:0000  27:0000  28:0000  29:0000  30:0000  31:0000
Port configuration for lport 0x08001000:
  enabled:                1
  loopback:               0
  link:                   0
  speed:                  0  max speed:               1000
  duplex:                 0
  linkscan:               2
  autonegotiate:          1
  master:                 2
  tx pause:               1  rx pause:                   1
  untagged vlan:          1
  vlan filter:            3
  stp state:              1
  learn:                  5
  discard:                0
  max frame size:      1522
  MC Disable SA:         no
  MC Disable TTL:        no
  MC egress untag:        0
  MC egress vid:          0
  MC TTL threshold:      -1
```

Table 10-2: Parameters in the output from the `show platform port` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ethernet MAC counters</strong></td>
<td></td>
</tr>
<tr>
<td>Combined receive/</td>
<td>Number of packets in each size range received and transmitted.</td>
</tr>
<tr>
<td>transmit packets by size (octets) counters</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>Number of 64 octet packets received and transmitted.</td>
</tr>
<tr>
<td>65 - 127</td>
<td>Number of 65 - 127 octet packets received and transmitted.</td>
</tr>
<tr>
<td>128 - 255</td>
<td>Number of 128 - 255 octet packets received and transmitted.</td>
</tr>
<tr>
<td>256 - 511</td>
<td>Number of 256 - 511 octet packets received and transmitted.</td>
</tr>
<tr>
<td>512 - 1023</td>
<td>Number of 512 - 1023 octet packets received and transmitted.</td>
</tr>
</tbody>
</table>
### Table 10-2: Parameters in the output from the `show platform port` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024 - MaxPktSz</td>
<td>Number of packets received and transmitted with size 1024 octets to the maximum packet length.</td>
</tr>
<tr>
<td>1519 - 1522</td>
<td>Number of 1519 - 1522 octet packets received and transmitted.</td>
</tr>
<tr>
<td>1519 - 2047</td>
<td>Number of 1519 - 2047 octet packets received and transmitted.</td>
</tr>
<tr>
<td>2048 - 4095</td>
<td>Number of 2048 - 4095 octet packets received and transmitted.</td>
</tr>
<tr>
<td>4096 - 9216</td>
<td>Number of 4096 - 9216 octet packets received and transmitted.</td>
</tr>
<tr>
<td>General Counters</td>
<td></td>
</tr>
<tr>
<td>Receive</td>
<td>Counters for traffic received.</td>
</tr>
<tr>
<td>Octets</td>
<td>Number of octets received.</td>
</tr>
<tr>
<td>Pkts</td>
<td>Number of packets received.</td>
</tr>
<tr>
<td>FCSErrors</td>
<td>Number of FCS (Frame Check Sequence) error events received.</td>
</tr>
<tr>
<td>UnicastPkts</td>
<td>Number of unicast packets received.</td>
</tr>
<tr>
<td>MulticastPkts</td>
<td>Number of multicast packets received.</td>
</tr>
<tr>
<td>BroadcastPkts</td>
<td>Number of broadcast packets received.</td>
</tr>
<tr>
<td>PauseMACCtlFrms</td>
<td>Number of Pause MAC Control Frames received.</td>
</tr>
<tr>
<td>OversizePkts</td>
<td>Number of oversize packets received.</td>
</tr>
<tr>
<td>Fragments</td>
<td>Number of fragments received.</td>
</tr>
<tr>
<td>Jabbers</td>
<td>Number of jabber frames received.</td>
</tr>
<tr>
<td>UnsupportOpcode</td>
<td>Number of MAC Control frames with unsupported opcode received.</td>
</tr>
<tr>
<td>AlignmentErrors</td>
<td>Receive Alignment Error Frame Counter.</td>
</tr>
<tr>
<td>SysErDurCarrier</td>
<td>Receive Code Error Counter.</td>
</tr>
<tr>
<td>CarrierSenseErr</td>
<td>Receive False Carrier Counter.</td>
</tr>
<tr>
<td>UndersizePkts</td>
<td>Number of undersized packets received.</td>
</tr>
<tr>
<td>Transmit</td>
<td>Counters for traffic transmitted.</td>
</tr>
</tbody>
</table>
Table 10-2: Parameters in the output from the `show platform port` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Octets</td>
<td>Number of octets transmitted.</td>
</tr>
<tr>
<td>Pkts</td>
<td>Number of packets transmitted.</td>
</tr>
<tr>
<td>UnicastPkts</td>
<td>Number of unicast packets transmitted.</td>
</tr>
<tr>
<td>MulticastPkts</td>
<td>Number of multicast packets transmitted.</td>
</tr>
<tr>
<td>BroadcastPkts</td>
<td>Number of broadcast packets transmitted.</td>
</tr>
<tr>
<td>PauseMACCtlFrms</td>
<td>Number of Pause MAC Control Frames transmitted.</td>
</tr>
<tr>
<td>OversizePkts</td>
<td>Number of oversize packets transmitted.</td>
</tr>
<tr>
<td>FrameWDeferrdTx</td>
<td>Transmit Single Deferral Frame counter.</td>
</tr>
<tr>
<td>FrmWExcesDefer</td>
<td>Transmit Multiple Deferral Frame counter.</td>
</tr>
<tr>
<td>SingleCollsnFrm</td>
<td>Transmit Single Collision Frame counter.</td>
</tr>
<tr>
<td>MultCollsnFrm</td>
<td>Transmit Multiple Collision Frame counter.</td>
</tr>
<tr>
<td>LateCollisions</td>
<td>Transmit Late Collision Frame counter.</td>
</tr>
<tr>
<td>ExcessivCollsns</td>
<td>Transmit Excessive Collision Frame counter.</td>
</tr>
<tr>
<td>Collisions</td>
<td>Transmit Total Collision counter</td>
</tr>
<tr>
<td><strong>Layer 3 Counters</strong></td>
<td></td>
</tr>
<tr>
<td>ifInUcastPkts</td>
<td>Inbound interface Unicast counter.</td>
</tr>
<tr>
<td>ifInDiscards</td>
<td>Inbound interface Discarded Packets counter.</td>
</tr>
<tr>
<td>ipInHdrErrors</td>
<td>Inbound interface Header Errors counter.</td>
</tr>
<tr>
<td>ifOutUcastPkts</td>
<td>Outbound interface Unicast counter.</td>
</tr>
<tr>
<td>ifOutErrors</td>
<td>Outbound interface Error counter.</td>
</tr>
<tr>
<td><strong>Miscellaneous Counters</strong></td>
<td></td>
</tr>
<tr>
<td>DropEvents</td>
<td>Drop Event counter</td>
</tr>
<tr>
<td>ifOutDiscards</td>
<td>Outbound interface Discarded Packets counter.</td>
</tr>
<tr>
<td>MTUExcdDiscard</td>
<td>Receive MTU Check Error Frame Counter</td>
</tr>
</tbody>
</table>
show port-security interface

**Overview**
Use this command to show the current port-security configuration and the switch port status.

**Syntax**
show port-security interface <port>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>The port to display information about. 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).</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
To see the port-security status on port1.0.1, use the following command:

```bash
awplus# show port-security interface port1.0.1
```

**Output**

Figure 10-14: 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 addresses : 1
Lock Status     : UNLOCKED
Security Violation Count : 0
Last Violation Source Address : None
```
show port-security intrusion

**Overview**
Shows the intrusion list. If the port is not specified, the entire intrusion table is shown.

**Syntax**
`show port-security intrusion [interface <port>]`

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interface</strong></td>
<td>Specify a port</td>
</tr>
<tr>
<td><strong>&lt;port&gt;</strong></td>
<td>The port to display information about. 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).</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
To see the intrusion list on port1.0.1, use the following command:

```
awplus# show port-security intrusion interface port1.0.1
```

**Output**
Figure 10-15: Example output from the `show port-security intrusion` command for port 1.0.1

```
Port Security Intrusion List
Interface: port1.0.1 -3 intrusion(s) detected
11-22-33-44-55-04 11-22-33-44-55-06 11-22-33-44-55-08
```
show storm-control

**Overview**  Use this command to display storm-control information for all interfaces or a particular interface.

**Syntax**  
```
show storm-control [<port>]
```

**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 10-16: Example output from the `show storm-control` command for port1.0.2

<table>
<thead>
<tr>
<th>Port</th>
<th>BcastLevel</th>
<th>McastLevel</th>
<th>DlfLevel</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.2</td>
<td>40.0%</td>
<td>100.0%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

**Example**  To display storm-control information for all ports, use the following command:

```
awplus# show storm-control
```
**Output**  
Figure 10-17: Example output from the `show storm-control` command for all ports

```
awplus#show storm-control
Port   BcastLevel McastLevel DlfLevel
port1.0.1 100.0%  100.0%  100.0%
port1.0.2 100.0%  100.0%  100.0%
port1.0.3 100.0%  100.0%  100.0%
port1.0.4 100.0%  100.0%  100.0%
port1.0.5 100.0%  100.0%  100.0%
port1.0.6 100.0%  100.0%  100.0%
port1.0.7 100.0%  100.0%  100.0%
port1.0.8 100.0%  100.0%  100.0%
port1.0.9 100.0%  100.0%  100.0%
port1.0.10 100.0% 100.0%  100.0%
port1.0.11 100.0%  100.0%  100.0%
port1.0.12 100.0%  100.0%  100.0%
port1.0.13 100.0%  100.0%  100.0%
port1.0.14 100.0%  100.0%  100.0%
port1.0.15 100.0%  100.0%  100.0%
port1.0.16 100.0%  100.0%  100.0%
port1.0.17 100.0%  100.0%  100.0%
port1.0.18 100.0%  100.0%  100.0%
port1.0.19 100.0%  100.0%  100.0%
port1.0.20 100.0%  100.0%  100.0%
port1.0.21 100.0%  100.0%  100.0%
port1.0.22 100.0%  100.0%  100.0%
port1.0.23 100.0%  100.0%  100.0%
port1.0.24 100.0%  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|10000|auto [10] [100] [1000] [10000]}
```

The following table shows the speed options for each type of port.

<table>
<thead>
<tr>
<th>Port type</th>
<th>Speed Options (units are Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RJ-45 and RJ.5copper ports</td>
<td>auto (default)</td>
</tr>
<tr>
<td></td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>supported tri-speed copper SFPs</td>
<td>auto (default)</td>
</tr>
<tr>
<td></td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>100Mb fiber SFPs</td>
<td>100</td>
</tr>
<tr>
<td>1000Mb fiber SFPs</td>
<td>auto (default)</td>
</tr>
<tr>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>10000Mb fiber SFP+</td>
<td>auto (default)</td>
</tr>
<tr>
<td></td>
<td>10000</td>
</tr>
</tbody>
</table>

**Mode**  Interface Configuration

**Default**  By default, ports autonegotiate speed (except for 100Base-FX ports which do not support auto-negotiation, so default to 100Mbps).

**Usage**  Switch ports in a static or dynamic (LACP) channel group must have the same port speed and be in full duplex mode. Once switch ports have been aggregated into a channel group, you can set the speed of all the switch ports in the channel group by applying this command to the channel group.

*NOTE:* Note that if multiple speeds are specified after the auto option to autonegotiate speeds, then only those speeds specified are attempted for autonegotiation.

**Examples**  To set the speed of a tri-speed port to 100Mbps, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# speed 100
```
To return the port to auto-negotiating its speed, enter the following commands:

```bash
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# speed auto
```

To set a port to auto-negotiate its speed at 100Mbps and 1000Mbps, enter the following commands:

```bash
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# speed auto 100 1000
```

To set a port to auto-negotiate its speed at 1000Mbps only, enter the following commands:

```bash
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# speed auto 1000
```

### Related Commands
- **duplex**
- **ecofriendly lpi**
- **polarity**
- **show interface**
- **speed (asyn)**
**storm-control level**

**Overview**  Use this command to specify the threshold level for broadcasting, multicast, or destination lookup failure (DLF) traffic for the port. Storm-control limits the specified traffic type to the specified threshold.

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>
nostorm-control {broadcast|multicast|dlf} level
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;level&gt;</code></td>
<td>&lt;0-100&gt; Specifies the threshold as a percentage of the maximum port speed.</td>
</tr>
<tr>
<td>broadcast</td>
<td>Applies the storm-control to broadcast frames.</td>
</tr>
<tr>
<td>multicast</td>
<td>Applies the storm-control to multicast frames.</td>
</tr>
<tr>
<td>dlf</td>
<td>Applies the storm-control to destination lookup failure traffic.</td>
</tr>
</tbody>
</table>

**Default**  By default, storm-control is disabled.

**Mode**  Interface Configuration

**Usage**  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.

**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
```
**Overview**

Enables the port-security feature. This feature is also known as the port-based learn limit. It allows the user to set the maximum number of MAC addresses that each port can learn.

Use the **no** variant of this command to disable the port-security feature.

**Syntax**

```
switchport port-security
no switchport port-security
```

**Mode**

Interface Configuration

**Examples**

To enable the port-security feature on port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# switchport port-security
```

To disable port-security feature on port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no switchport port-security
```
switchport port-security aging

**Overview** Sets the port-security MAC to time out.

Use the `no` variant of this command to set the port-security to not time out.

**Syntax**

- `switchport port-security aging`
- `no switchport port-security aging`

**Mode** Interface Configuration

**Examples** To set the MAC to time out, use the following command:

```
awplus# switchport port-security aging
```

To unset the MAC time out, use the following command:

```
awplus# no switchport port-security aging
```
**switchport port-security maximum**

**Overview** Sets the maximum MAC address that each port can learn.

Use the **no** variant of this command to unset the maximum number of MAC addresses that each port can learn. This is same as setting the maximum number to 0. This command also resets the intrusion list table.

If a new MAC is seen on a port with port security enabled and the MAC is statically configured for another port, a violation is triggered. The maximum learn limit will be ignored and the specified intrusion action for the port will be carried out.

**Syntax**

```plaintext
switchport port-security maximum <0-256>
no switchport port-security maximum
```

**Mode** Interface Configuration

**Examples**

To learn 3 MAC addresses on port1.0.4, use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# switchport port-security maximum 3
```

To remove the MAC learning limit on port1.0.4, use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no switchport port-security maximum
```
**switchport port-security violation**

**Overview**  
Sets the violation action for a switch port when the port exceeds the learning limits. The port action can be either **shutdown**, **restrict** or **protect**. If **shutdown** is set, the physical link will be disabled and “shutdown” will be shown in the config. If **restrict** is set, the packet from the un-authorized MAC will be discarded and SNMP TRAP will be generated to alert management. If **protect** is set, the packet will simply be discarded by the packet processor silently.

The **no** variant of this command sets the violation action to default. The default violation action is **protect**.

**Syntax**  
```
switchport port-security violation {shutdown|restrict|protect}
no switchport port-security violation
```

**Mode**  
Interface Configuration

**Examples**  
To set the action to be **shutdown** on port1.0.4, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# switchport port-security violation shutdown
```

To set the port-security action to the default (**protect**) on port1.0.4, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no switchport port-security violation
```
thrash-limiting

### Overview
Sets and configures the thrash limit action that will be applied to any port on the device when a thrashing condition is detected. The thrash-limiting timeout specifies the time, in seconds, for which the thrash action is employed.

### Syntax
```plaintext
thrash-limiting {[action
{learn-disable|link-down|port-disable|vlan-disable|none}]
[timeout <0-86400>]} 
no thrash-limiting {action|timeout}
```

### Default
The default action is learn-disable.

### Mode
Interface Configuration

### Usage
See the “Thrash Limiting” section in the Switching Feature Overview and Configuration Guide for relevant conceptual, configuration, and overview information prior to applying this command.

### Examples
To set the action to learn disable for port1.0.4, use the following commands:
```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# thrash-limiting action learn-disable
```
To block all traffic on a vlan, use the following command:
```plaintext
awplus# configure terminal
awplus(config)# thrash-limiting action vlan-disable
```
To set the thrash limiting timeout to 5 seconds, use the following command:
```plaintext
awplus(config-if)# thrash-limiting timeout 5
```
To set the thrash limiting action to its default, use the following command:
```
awplus(config-if)# no thrash-limiting action
```

To set the thrash limiting timeout to its default, use the following command:
```
awplus(config-if)# no thrash-limiting timeout
```

**Related Commands**
- `loop-protection`
- `loop-protection action`
- `loop-protection timeout`
- `show loop-protection`
undebug loopprot

**Overview**  This command applies the functionality of the no debug loopprot command.
**overview**  This command applies the functionality of the no **debug platform packet** command.
11 VLAN Commands

Introduction

Overview  This chapter provides an alphabetical reference of commands used to configure VLANs. For more information see the VLAN Feature Overview and Configuration Guide.
VLAN COMMANDS

Command List

• “clear vlan statistics” on page 446
• “port-vlan-forwarding-priority” on page 447
• “private-vlan” on page 450
• “private-vlan association” on page 451
• “show port-vlan-forwarding-priority” on page 452
• “show vlan” on page 453
• “show vlan classifier group” on page 454
• “show vlan classifier group interface” on page 455
• “show vlan classifier interface group” on page 456
• “show vlan classifier rule” on page 457
• “show vlan private-vlan” on page 458
• “show vlan statistics” on page 459
• “switchport access vlan” on page 460
• “switchport enable vlan” on page 461
• “switchport mode access” on page 462
• “switchport mode private-vlan” on page 463
• “switchport mode private-vlan trunk promiscuous” on page 464
• “switchport mode private-vlan trunk secondary” on page 466
• “switchport mode trunk” on page 468
• “switchport private-vlan host-association” on page 469
• “switchport private-vlan mapping” on page 470
• “switchport trunk allowed vlan” on page 471
• “switchport trunk native vlan” on page 474
• “switchport vlan-stacking (double tagging)” on page 476
• “switchport voice dscp” on page 477
• “switchport voice vlan” on page 478
• “switchport voice vlan priority” on page 481
• “vlan” on page 482
• “vlan classifier activate” on page 483
• “vlan classifier group” on page 484
• “vlan classifier rule ipv4” on page 485
• “vlan classifier rule proto” on page 486
• “vlan database” on page 489
• “vlan mode stack-local-vlan” on page 490
• “vlan statistics” on page 492
clear vlan statistics

**Overview**
This command resets the counters for either a specific VLAN statistics instance or (by not specifying an instance) resets the counters for all instances.

The terms **frame** and **packet** are used interchangeably.

**Syntax**
clear vlan statistics [name <instance_name>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan statistics</td>
<td>The count of incoming frames or bytes collected on a per VLAN basis.¹</td>
</tr>
<tr>
<td>&lt;instance-name&gt;</td>
<td>The name of the instance for which incoming frames and their bytes are counted.¹</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Examples**
To reset all packet counters for the packet counter instance **vlan2-data**:

```
awplus# clear vlan statistics name vlan2-data
```

To reset all packet counters for all packet counter instances.

```
awplus# clear vlan statistics
```

**Related Commands**
show vlan statistics

vlan statistics
**Overview**

Use this command to set the highest priority protocol to control transitions from blocking to forwarding traffic. This command prioritizes switch port forwarding mode control, when more than one of EPSR, Loop Protection, and MAC thrashing protection protocols are used on the switch.

EPSR, Loop Protection and MAC Thrashing use the same mechanism to block or forward traffic. This command sets the highest priority protocol to control transitions from blocking to forwarding traffic. Setting the priority stops contention between protocols.

For example, if EPSR is set to the highest priority protocol to block traffic on vlan10 on port1.0.2 then this stops MAC Thrashing from forwarding traffic on vlan10 on port1.0.2.

**CAUTION:**

*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.
one | Sets the protocols to have equal priority. This was the previous behavior before this command was added, and allows protocols to override each other to set a port to forwarding a VLAN. Note that this option must not be set on a EPSR master node. Use the epsr parameter option on an EPSR master node to avoid unexpected broadcast storms.

**Default**

By default, the highest priority protocol is EPSR

**Mode**

Global Configuration
**Usage**

EPSR, Loop Protection and MAC Thrashing protection do not usually need to be configured on a switch, because they perform similar functions—each prevents network loops by blocking a selected port for each (loop containing) VLAN.

However, if more than one of these three features is configured on a switch, you can use this command to prioritize either EPSR or Loop Protection when their effects on a port would conflict and override each other. Previously, each protocol could set a port to forwarding for a VLAN, sometimes overriding the previous setting by another protocol to block the port. This could sometimes lead to unexpected broadcast storms.

Now, when a protocol is set to have the highest priority over a data VLAN on a port, it will not allow other protocols to put that port-vlan into a forwarding state if the highest priority protocol blocked it.

The priority mechanism is only used for blocking-to-forwarding transitions; protocols remain independent on the forwarding-to-blocking transitions.

For example, with an EPSR master node in a two-node ESPR ring with the below settings:

- The EPSR master node primary port is configured to switchport interface port1.0.1
- The EPSR master node secondary port is configured to switchport interface port1.0.2
- The EPSR master node control VLAN is configured to VLAN interface vlan10
- The EPSR master node has a first data VLAN configured to VLAN interface vlan20
- The EPSR master node has a second data VLAN configured to VLAN interface vlan30.

Initially, the EPSR ring is complete, with port1.0.2 blocking data VLANs vlan20 and vlan30 and some broadcast traffic flowing through. If the user removes vlan30 from EPSR, a storm is created on vlan30. MAC thrashing protection detects it and blocks vlan30.

Then after the storm has stopped, MAC thrashing protection sets it to forwarding again and it keeps oscillating between forwarding and blocking. In the meantime, the user adds back vlan30 to EPSR as a data VLAN and EPSR blocks it on port1.0.2.

If the priority is set to none (``port-vlan-forwarding-priority none``), MAC thrashing protection notices that the storm has stopped again and decides to put vlan30 on port1.0.2 into forwarding state. This overrides what EPSR requires for this port-VLAN and creates a storm. This matches the old behavior before this feature was implemented.

If the priority is set to EPSR or default (``port-vlan-forwarding-priority epsr``), MAC thrashing protection notices that the storm has stopped again and attempts to put vlan30 on port1.0.2 into forwarding state. The higher priority protocol (EPSR) is blocking the VLAN on this port, so it stays blocking and no storm occurs.
VLAN COMMANDS
PORT-VLAN-FORWARDING-PRIORITY

Example
To prioritize EPSR over Loop Protection or MAC Thrashing protection settings, so that Loop Protection or MAC Thrashing protection cannot set a port to the forwarding state a VLAN if EPSR has set it to the blocking state, use the commands:

awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority epsr

To prioritize Loop Protection over EPSR or MAC Thrashing protection settings, so that EPSR or MAC Thrashing protection cannot set a port to the forwarding state a VLAN if Loop Protection has set it to the blocking state, use the commands:

awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority loop-protection

To set EPSR, Loop Protection, and MAC Thrashing protection protocols to have equal priority for port forwarding and blocking, which allows the protocols to override each other to set a port to the forwarding or blocking states, use the commands:

awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority none

To restore the default highest priority protocol back to the default of EPSR, use the commands:

awplus# configure terminal
awplus(config)# no port-vlan-forwarding-priority

Related Commands
show port-vlan-forwarding-priority
private-vlan

**Overview**
Use this command to create a private VLAN. Private VLANs can be either primary or secondary. Secondary VLANs can be either community or isolated.

Use the `no` variant of this command to remove the specified private VLAN.

For more information, see the VLAN Feature Overview and Configuration Guide.

**Syntax**

```
private-vlan <vlan-id> {community|isolated|primary}
no private-vlan <vlan-id> {community|isolated|primary}
```

**Mode**
VLAN Configuration

**Examples**

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2 name vlan2 state enable
awplus(config-vlan)# vlan 3 name vlan3 state enable
awplus(config-vlan)# vlan 4 name vlan4 state enable
awplus(config-vlan)# private-vlan 2 primary
awplus(config-vlan)# private-vlan 3 isolated
awplus(config-vlan)# private-vlan 4 community
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no private-vlan 2 primary
awplus(config-vlan)# no private-vlan 3 isolated
awplus(config-vlan)# no private-vlan 4 community
```
**private-vlan association**

**Overview**

Use this command to associate a secondary VLAN to a primary VLAN. Only one isolated VLAN can be associated to a primary VLAN. Multiple community VLANs can be associated to a primary VLAN.

Use the `no` variant of this command to remove association of all the secondary VLANs to a primary VLAN.

For more information, see the VLAN Feature Overview and Configuration Guide.

**Syntax**

```
private-vlan <primary-vlan-id> association {add <secondary-vlan-id>|remove <secondary-vlan-id>}
no private-vlan <primary-vlan-id> association
```

**Mode**

VLAN Configuration

**Examples**

The following commands associate primary VLAN 2 with secondary VLAN 3:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 2 association add 3
```

The following commands remove the association of primary VLAN 2 with secondary VLAN 3:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 2 association remove 3
```

The following commands remove all secondary VLAN associations of primary VLAN 2:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no private-vlan 2 association
```
**show port-vlan-forwarding-priority**

**Overview**  Use this command to display the highest priority protocol that controls port-vlan forwarding or blocking traffic. This command displays whether EPSR or Loop Protection is set as the highest priority for determining whether a port forwards a VLAN, as set by the `port-vlan-forwarding-priority` command. For more information about EPSR, see the EPSR Feature Overview and Configuration Guide.

**Syntax**  `show port-vlan-forwarding-priority`

**Mode**  Privileged Exec

**Example**  To display the highest priority protocol, use the command:

```bash
awplus# show port-vlan-forwarding-priority
```

**Output**  Example output from the `show port-vlan-forwarding-priority` command

```
Port-vlan Forwarding Priority: EPSR
```

**Related Commands**  `port-vlan-forwarding-priority`
show vlan

**Overview**  Use this command to display information about a particular VLAN by specifying the VLAN ID. It displays information for all the VLANs configured.

**Syntax**  `show vlan {all|brief|dynamic|static|auto|static-ports <1-4094>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4094&gt;</td>
<td>Display information about the VLAN specified by the VLAN ID.</td>
</tr>
<tr>
<td>all</td>
<td>Display information about all VLANs on the device.</td>
</tr>
<tr>
<td>brief</td>
<td>Display information about all VLANs on the device.</td>
</tr>
<tr>
<td>dynamic</td>
<td>Display information about all VLANs learned dynamically.</td>
</tr>
<tr>
<td>static</td>
<td>Display information about all statically configured VLANs.</td>
</tr>
<tr>
<td>auto</td>
<td>Display information about all auto-configured VLANs.</td>
</tr>
<tr>
<td>static-ports</td>
<td>Display static egress/forbidden ports.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**  To display information about VLAN 2, use the command:

```
awplus# show vlan 2
```

**Output**  Figure 11-2: Example output from the `show vlan` command

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
<th>Type</th>
<th>State</th>
<th>Member ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>VLAN0002</td>
<td>STATIC</td>
<td>ACTIVE</td>
<td>port1.0.3(u) port1.0.4(u) port1.0.5(u) port1.0.6(u)</td>
</tr>
</tbody>
</table>

**Related Commands**  `vlan`
show vlan classifier group

**Overview**
Use this command to display information about all configured VLAN classifier groups or a specific group.

**Syntax**
show vlan classifier group [1-16]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-16</td>
<td>VLAN classifier group identifier</td>
</tr>
</tbody>
</table>

**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>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;switch-port&gt;</td>
<td>Specify the switch port interface classifier group identifier</td>
</tr>
</tbody>
</table>

Mode
User Exec and Privileged Exec

Usage
All configured VLAN classifier groups are shown for a single interface.

Example
To display VLAN classifier group information for switch port interface port1.0.2, enter the command:

```bash
awplus# show vlan classifier group interface port1.0.2
```

Output
Figure 11-3: Example output from the `show vlan classifier group interface port1.0.1` command:

```
vlan classifier group 1 interface port1.0.1
```

Related Commands
- `vlan classifier group`
- `show vlan classifier interface group`
show vlan classifier interface group

Overview
Use this command to display information about all interfaces configured for a VLAN group or all the groups.

Syntax
show vlan classifier interface group [1-16]

Mode
User Exec and Privileged Exec

Usage
If a group ID is not specified, all interfaces configured for all VLAN classifier groups are shown. If a group ID is specified, the interfaces configured for this VLAN classifier group are shown.

Example
To display information about all interfaces configured for all VLAN groups, enter the command:

awplus# show vlan classifier interface group

To display information about all interfaces configured for VLAN group 1, enter the command:

awplus# show vlan classifier interface group 1

Output
Figure 11-4: Example output from the show vlan classifier interface group command

```
vlan classifier group 1 interface port1.0.1
vlan classifier group 1 interface port1.0.2
vlan classifier group 2 interface port1.0.3
vlan classifier group 2 interface port1.0.4
```

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**  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-256&gt;</code></td>
<td>VLAN classifier rule identifier</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Usage**  If a rule ID is not specified, all configured VLAN classifier rules are shown. If a rule ID is specified, a specific configured VLAN classifier rule is shown.

**Example**  To display information about VLAN classifier rule 1, enter the command:

```
awplus# show vlan classifier rule 1
```

**Output**  

*Figure 11-6: Example output from the `show vlan classifier rule` command*

```
vlan classifier group 1 add rule 1
```

**Related Commands**  
- `vlan classifier activate`
- `vlan classifier rule ipv4`
- `vlan classifier rule proto`
show vlan private-vlan

**Overview**  Use this command to display the private VLAN configuration and associations.

**Syntax**  
```
show vlan private-vlan
```

**Mode**  User Exec and Privileged Exec

**Example**  
To display the private VLAN configuration and associations, enter the command:
```
awplus# show vlan private-vlan
```

**Output**  
Figure 11-7: Example output from the `show vlan private-vlan` command

<table>
<thead>
<tr>
<th>PRIMARY</th>
<th>SECONDARY</th>
<th>TYPE</th>
<th>INTERFACES</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>isolated</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>community</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>isolated</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**
- `private-vlan`
- `private-vlan association`
show vlan statistics

**Overview**  
Use this command to display the current configuration for either a specific VLAN statistics instance, or (by not specifying an instance) display all VLAN packet counter instances.

**Syntax**  
`show vlan statistics [name <instance_name>]`

**Mode**  
User Exec and Privileged Exec

**Examples**  
To display all packet counters for the packet counter instance `vlan2-data`

```
awplus# show vlan statistics name vlan2-data
```

To display all packet counters for all packet counter instances.

```
awplus# show vlan statistics
```

**Table 11-1: Example output from the `show vlan statistics` command**

```
VLAN Stats Collection: vlan2-data
VLAN ID: 2
Port Map: port1.0.1, port1.0.2, port1.0.4
Ingress Packets: total 941, bytes 66185
```
**switchport access vlan**

**Overview**  
Use this command to change the port-based VLAN of the current port.  
Use the no variant of this command to change the port-based VLAN of this port to the default VLAN, vlan1.

**Syntax**  
```plaintext
switchport access vlan <vlan-id>
no switchport access vlan
```

**Default**  
Reset the default VLAN 1 to specified switchports using the negated form of this command.

**Mode**  
Interface Configuration

**Usage**  
Any untagged frame received on this port will be associated with the specified VLAN.

**Examples**  
To change the port-based VLAN to VLAN 3 for port1.0.2, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport access vlan 3
```
To reset the port-based VLAN to the default VLAN 1 for port1.0.2, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport access vlan
```

**Validation Command**  
`show interface switchport`

**Related Commands**  
`show vlan`
**switchport enable vlan**

**Overview**  This command enables the VLAN on the port manually once disabled by certain actions, such as QSP (QoS Storm Protection) or EPSR (Ethernet Protection Switching Ring). Note that if the VID is not given, all disabled VLANs are re-enabled.

**Syntax**  
```
switchport enable vlan [<1-4094>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Re-enables the VLAN on the port.</td>
</tr>
<tr>
<td>&lt;1-4094&gt;</td>
<td>VLAN ID.</td>
</tr>
</tbody>
</table>

**Mode**  Interface Configuration

**Example**  To re-enable the **port1.0.1** from VLAN 1:
```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport enable vlan 1
```

**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}]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ingress-filter</td>
<td>Set the ingress filtering for the received frames.</td>
</tr>
<tr>
<td>enable</td>
<td>Turn on ingress filtering for received frames. This is the default.</td>
</tr>
<tr>
<td>disable</td>
<td>Turn off ingress filtering to accept frames that do not meet the classification criteria.</td>
</tr>
</tbody>
</table>

**Default**  By default, ports are in access mode with ingress filtering on.

**Usage**  Use access mode to send untagged frames only.

**Mode**  Interface Configuration

**Example**  
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access ingress-filter enable
```

**Validation Command**  show interface switchport
**switchport mode private-vlan**

**Overview**  
Use this command to make a Layer 2 port a private VLAN host port or a promiscuous port.

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

**Syntax**
```
switchport mode private-vlan {host|promiscuous}
no switchport mode private-vlan {host|promiscuous}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>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.</td>
</tr>
<tr>
<td>promiscuous</td>
<td>A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN.</td>
</tr>
</tbody>
</table>

**Mode**  
Interface Configuration

**Examples**
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode private-vlan host
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode private-vlan promiscuous
awplus(config)# interface port1.0.4
awplus(config-if)# no switchport mode private-vlan promiscuous
```

**Related Commands**
switchport private-vlan mapping
switchport mode private-vlan trunk promiscuous

**Overview**  Use this command to enable a port in trunk mode to be promiscuous port for isolated VLANs.

*NOTE:* Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. Private VLAN trunk ports and GVRP are mutually exclusive.

Use the no variant of this command to remove a port in trunk mode as a promiscuous port for isolated VLANs. You must first remove the secondary port, or ports, in trunk mode associated with the promiscuous port with the no switchport mode private-vlan trunk secondary command.

**Syntax**

```
switchport mode private-vlan trunk promiscuous group <group-id>
no switchport mode private-vlan trunk promiscuous
```

**Parameter** | **Description**
--- | ---
<group-id> | The group ID is a numeric value in the range 1 to 32 that is used to associate the promiscuous port with secondary ports.

**Default**  By default, a port in trunk mode is disabled as a promiscuous port.

**Mode**  Interface Configuration

**Usage**  A port must be put in trunk mode with switchport mode trunk command before it can be enabled as a promiscuous port.

To add VLANs to be trunked over the promiscuous port, use the switchport trunk allowed vlan command. These VLANs can be isolated VLANs, or non-private VLANs.

To configure the native VLAN for the promiscuous port, use the switchport trunk native vlan command. The native VLAN can be an isolated VLAN, or a non-private VLAN.

When you enable a promiscuous port, all of the secondary port VLANs associated with the promiscuous port via the group ID number must be added to the promiscuous port. In other words, the set of VLANs on the promiscuous port must be a superset of all the VLANs on the secondary ports within the group.

**Examples**  To create the isolated VLANs 2, 3 and 4 and then enable port1.0.2 in trunk mode as a promiscuous port for these VLANs with the group ID of 3, use the following commands:
To create the isolated VLANs 2, 3 and 4 and then enable port1.1.2 in trunk mode as a promiscuous port for these VLANs with the group ID of 3, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2-4
awplus(config-vlan)# private-vlan 2 isolated
awplus(config-vlan)# private-vlan 3 isolated
awplus(config-vlan)# private-vlan 4 isolated
awplus(config-vlan)# exit
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 2-4
awplus(config-if)# switchport mode private-vlan trunk promiscuous group 3
```

To remove port1.0.2 in trunk mode as a promiscuous port for a private VLAN, use the commands:

```
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`
VLAN COMMANDS
SWITCHPORT MODE PRIVATE-VLAN TRUNK SECONDARY

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;group-id&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

Default
By default, a port in trunk mode is disabled as a secondary port.

When a port in trunk mode is enabled to be a secondary port for isolated VLANs, by default it will have a native VLAN of none (no native VLAN specified).

Mode
Interface Configuration

Usage
A port must be put in trunk mode with switchport mode trunk command before the port is enabled as a secondary port in trunk mode.

To add VLANs to be trunked over the secondary port use the switchport trunk allowed vlan command. These must be isolated VLANs and must exist on the associated promiscuous port.

To configure the native VLAN for the secondary port, use the switchport trunk native vlan command. The native VLAN must be an isolated VLAN and must exist on the associated promiscuous port.

Examples
To create isolated private VLAN 2 and then enable port1.0.3 in trunk mode as a secondary port for the this VLAN with the group ID of 3, use the following commands:
To create isolated private VLAN 2 and then enable port1.1.3 in trunk mode as a secondary port for the this VLAN with the group ID of 3, use the following commands:

```bash
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2
awplus(config-vlan)# private-vlan 2 isolated
awplus(config-vlan)# exit
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 2
awplus(config-if)# switchport mode private-vlan trunk secondary group 3
```

To remove port1.1.3 in trunk mode as a secondary port, use the commands:

```bash
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no switchport mode private-vlan trunk secondary
```

Related Commands

- switchport mode private-vlan trunk promiscuous
- switchport mode trunk
- switchport trunk allowed vlan
- switchport trunk native vlan
- show vlan private-vlan
**switchport mode trunk**

**Overview**
Use this command to set the switching characteristics of the port to trunk. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

**Syntax**
```plaintext
switchport mode trunk [ingress-filter {enable|disable}]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ingress-filter</td>
<td>Set the ingress filtering for the frames received.</td>
</tr>
<tr>
<td>enable</td>
<td>Turn on ingress filtering for received frames. This is the default.</td>
</tr>
<tr>
<td>disable</td>
<td>Turn off ingress filtering to accept frames that do not meet the classification criteria.</td>
</tr>
</tbody>
</table>

**Default**
By default, ports are in access mode, are untagged members of the default VLAN (vlan1), and have ingress filtering on.

**Mode**
Interface Configuration

**Usage**
A port in trunk mode can be a tagged member of multiple VLANs, and an untagged member of one native VLAN.

To configure which VLANs this port will trunk for, use the switchport trunk allowed vlan command.

**Example**
```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode trunk ingress-filter enable
```

**Validation Command**
show interface switchport
VLAN COMMANDS
SWITCHPORT PRIVATE-VLAN HOST-ASSOCIATION

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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;primary-vlan-id&gt;</td>
<td>VLAN ID of the primary VLAN.</td>
</tr>
<tr>
<td>&lt;secondary-vlan-id&gt;</td>
<td>VLAN ID of the secondary VLAN (either isolated or community).</td>
</tr>
</tbody>
</table>

**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
```
VLAN COMMANDS

SWITCHPORT PRIVATE-VLAN MAPPING

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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;primary-vlan-id&gt;</code></td>
<td>VLAN ID of the primary VLAN.</td>
</tr>
<tr>
<td><code>&lt;secondary-vid-list&gt;</code></td>
<td>VLAN ID of the secondary VLAN (either isolated or community), or a range of VLANs, or a comma-separated list of VLANs and ranges.</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration

**Usage**
This command can be applied to a switch port or a static channel group, but not a dynamic (LACP) channel group. LACP channel groups (dynamic/LACP aggregators) cannot be promiscuous ports in private VLANs.

**Examples**
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport private-vlan mapping 2 add 3-4
awplus(config-if)# switchport private-vlan mapping 2 remove 3-4
awplus(config-if)# no switchport private-vlan mapping
```

**Related Commands**
switchport mode private-vlan
VLAN Commands

Switchport Trunk Allowed VLAN

**Overview**

Use this command to add VLANs to be trunked over this switch port. Traffic for these VLANs can be sent and received on the port.

Use the no variant of this command to reset switching characteristics of a specified interface to negate a trunked configuration specified with switchport trunk allowed vlan command.

**Syntax**

```
switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add <vid-list>
switchport trunk allowed vlan remove <vid-list>
switchport trunk allowed vlan except <vid-list>
no switchport trunk
```

**Parameter** | **Description**
--- | ---
all | Allow all VLANs to transmit and receive through the port.
none | Allow no VLANs to transmit and receive through the port.
add | Add a VLAN to transmit and receive through the port. Only use this parameter if a list of VLANs are already configured on a port.
remove | Remove a VLAN from transmit and receive through the port. Only use this parameter if a list of VLANs are already configured on a port.
except | All VLANs, except the VLAN for which the VID is specified, are part of its port member set. Only use this parameter to remove VLANs after either this parameter or the 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 (vlan1).

**Mode**

Interface Configuration

**Usage**

The all parameter sets the port to be a tagged member of all the VLANs configured on the device. The none parameter removes all VLANs from the port’s tagged member set. The add and remove parameters will add and remove VLANs to and from the port’s member set. See the note below about restrictions when using the add, remove, except, and all parameters.
**NOTE:** Only use the *add* or the *remove* parameters with this command if a list of VLANs are configured on a port. Only use the *except* parameter to remove VLANs after either the *except* or the *all* parameters have first been used to add a list of VLANs to a port.

To remove a VLAN, where the configuration for port 1.0.6 shows the below output:

```
awplus#show running-config
! interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 4
```

Remove VLAN 3 by re-entering the *except* parameter with the list of VLANs to remove, instead of using the *remove* parameter, as shown in the command example below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# switchport trunk allowed vlan except 3,4
```

Then the configuration is changed after entering the above commands to remove VLAN 3:

```
awplus#show running-config
! interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 3-4
```

To add a VLAN, where the configuration for port 1.0.6 shows the below output:

```
awplus#show running-config
! interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 3-5
```
Add VLAN 4 by re-entering the `except` parameter with a list of VLANs to exclude, instead of using the `add` parameter to include VLAN 4, as shown in the command example below:

```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport trunk allowed vlan except 3,5
```

The configuration is changed after entering the above commands to add VLAN 4:

```
awplus# show running-config

!  
interface port1.0.5
switchport
switchport mode trunk
switchport trunk allowed vlan except 3,5
```

**Examples**

The following shows adding a single VLAN to the port’s member set.

```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2
```

The following shows adding a range of VLANs to the port’s member set.

```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2-4
```

The following shows adding a list of VLANs to the port’s member set.

```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2,3,4
```
### switchport trunk native vlan

**Overview**  Use this command to configure the native VLAN for this port. The native VLAN is used for classifying the incoming untagged packets. Use the `none` parameter with this command to remove the native VLAN from the port and set the acceptable frame types to vlan-tagged only.

Use the `no` variant of this command to revert the native VLAN to the default VLAN ID 1. Command negation removes tagged VLANs, and sets the native VLAN to the default VLAN.

**Syntax**  
```
switchport trunk native vlan {<vid>|none}
no switchport trunk native vlan
```

**Parameter** | **Description**
--- | ---
`<vid>` | <2-4094>
The ID of the VLAN that will be used to classify the incoming untagged packets. The VLAN ID must be a part of the VLAN member set of the port.

`none` | No native VLAN specified. This option removes the native VLAN from the port and sets the acceptable frame types to vlan-tagged only. Note: Use the `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**  The following commands show configuration of VLAN 2 as the native VLAN for interface `port1.0.2`:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk native vlan 2
```

The following commands show the removal of the native VLAN for interface `port1.0.2`:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk native vlan none
```
The following commands revert the native VLAN to the default VLAN 1 for interface port1.0.2:

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport trunk native vlan
### switchport vlan-stacking (double tagging)

**Overview**  
Use this command to enable VLAN stacking on a port and set it to be a customer-edge-port or provider-port. This is sometimes referred to as VLAN double-tagging, nested VLANs, or QinQ.

Use the `no` parameter with this command to disable VLAN stacking on an interface.

**Syntax**
```
switchport vlan-stacking {customer-edge-port|provider-port}
no switchport vlan-stacking
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer-edge-port</td>
<td>Set the port to be a customer edge port. This port must already be in access mode.</td>
</tr>
<tr>
<td>provider-port</td>
<td>Set the port to be a provider port. This port must already be in trunk mode.</td>
</tr>
</tbody>
</table>

**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.

Traffic with an extra VLAN header added by VLAN stacking cannot be routed.

**Example**
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport vlan-stacking customer-edge-port
```
switchport voice dscp

**Overview**  
Use this command to configure the Layer 3 DSCP value advertised when the transmission of LLDP-MED Network Policy TLVs for voice devices is enabled. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified DSCP value.

Use the **no** variant of this command to reset the DSCP value to the default, 0.

**Syntax**
```
switchport voice dscp <0–63>
no switchport voice dscp
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dscp</td>
<td>Specify a DSCP value for voice data.</td>
</tr>
<tr>
<td>&lt;0–63&gt;</td>
<td>DSCP value.</td>
</tr>
</tbody>
</table>

**Default**  
A DSCP value of 0 will be advertised.

**Mode**  
Interface Configuration

**Usage**  
LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (**lldp run** command)
- Voice VLAN is configured for the port (**switchport voice vlan** command)
- The port is configured to transmit LLDP advertisements—enabled by default (**lldp transmit receive** command)
- The port is configured to transmit Network Policy TLVs—enabled by default (**lldp med-tlv-select** command)
- There is an LLDP-MED device connected to the port

**Example**
```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport voice dscp 27
```

**Related Commands**
```
lldp med-tlv-select
show lldp
switchport voice vlan
```
switchport voice vlan

**Overview**  Use this command to configure the Voice VLAN tagging advertised when the transmission of LLDP-MED Network Policy TLVs for voice endpoint devices is enabled. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified tagging. This command also sets the ports to be spanning tree edge ports, that is, it enables spanning tree portfast on the ports.

Use the no variant of this command to remove LLDP-MED network policy configuration for voice devices connected to these ports. This does not change the spanning tree edge port status.

**Syntax**

```
switchport voice vlan [<vid>|dot1p|dynamic|untagged]
no switchport voice vlan
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vid&gt;</td>
<td>VLAN identifier, in the range 1 to 4094.</td>
</tr>
<tr>
<td>dot1p</td>
<td>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.)</td>
</tr>
<tr>
<td>dynamic</td>
<td>The VLAN ID with which the IP phone should send tagged packets will be assigned by RADIUS authentication.</td>
</tr>
<tr>
<td>untagged</td>
<td>The IP phone should send untagged packets.</td>
</tr>
</tbody>
</table>

**Default**  By default, no Voice VLAN is configured, and therefore no network policy is advertised for voice devices.

**Mode**  Interface Configuration

**Usage**  LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (lldp run command)
- Voice VLAN is configured for the port using this command (switchport voice vlan)
- The port is configured to transmit LLDP advertisements—enabled by default (lldp transmit receive command)
- The port is configured to transmit Network Policy TLVs—enabled by default (lldp med-tlv-select command)
- There is an LLDP-MED device connected to the port.

To set the priority value to be advertised for tagged frames, use the switchport voice vlan priority command.
If the Voice VLAN details are to be assigned by RADIUS, then the RADIUS server must be configured to send the attribute “Egress-VLANID (56)” or “Egress-VLAN-Name (58)” in the RADIUS Accept message when authenticating a phone attached to this port.

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 `port1.0.5` to send voice data tagged for VLAN 10, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport voice vlan 10
```

To tell IP phones connected to ports `1.0.2-1.0.6` to send priority tagged packets (802.1p priority tagged with VID 0, so that they will be assigned to the port VLAN) use the following commands. The priority value is 5 by default, but can be configured with the `switchport voice vlan priority` command.

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.6
awplus(config-if)# switchport voice vlan dot1p
```

To dynamically configure the VLAN ID advertised to IP phones connected to `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 `port1.0.6`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no switchport voice vlan
```
**Related Commands**

- egress-vlan-id
- egress-vlan-name
- lldp med-tlv-select
- spanning-tree edgeport (RSTP and MSTP)
- switchport voice dscp
- switchport voice vlan priority
- show lldp
**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 port 1.0.6, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no switchport voice vlan
```

**Related Commands**

- `lldp med-tlv-select`
- `show lldp`
- `switchport voice vlan`
VLAN COMMANDS
VLAN

**Overview**  This command creates VLANs, assigns names to them, and enables or disables them. Specifying the `disable` state causes all forwarding over the specified VLAN ID to cease. Specifying the `enable` state allows forwarding of frames on the specified VLAN.

The **no** variant of this command destroys the specified VLANs.

**Syntax**

```
vlan <vid> [name <vlan-name>] [state {enable|disable}]
vlan <vid-range> [state {enable|disable}]
vlan {<vid>|<vlan-name>} [mtu <mtu-value>]
no vlan {<vid>|<vid-range>} [mtu]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;vid&gt;</code></td>
<td>The VID of the VLAN to enable or disable in the range <code>&lt;1-4094&gt;</code>.</td>
</tr>
<tr>
<td><code>&lt;vlan-name&gt;</code></td>
<td>The ASCII name of the VLAN. Maximum length: 32 characters.</td>
</tr>
<tr>
<td><code>&lt;vid-range&gt;</code></td>
<td>Specifies a range of VLAN identifiers.</td>
</tr>
<tr>
<td><code>&lt;mtu-value&gt;</code></td>
<td>Specifies the Maximum Transmission Unit (MTU) size in bytes, in the range 68 to 1500 bytes, for the VLAN.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Sets VLAN into an enable state.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Sets VLAN into a disable state.</td>
</tr>
</tbody>
</table>

**Default**  By default, VLANs are enabled when they are created.

**Mode**  VLAN Configuration

**Examples**

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 45 name accounts state enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 45
```

**Related Commands**

- `mtu`
- `vlan database`
- `show vlan`
VLAN COMMANDS
VLAN CLASSIFIER ACTIVATE

**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>
```

**Mode**
Interface Configuration mode for a switch port.

**Usage**
See the protocol-based VLAN configuration example in the VLAN Feature Overview and Configuration Guide for configuration details.

**Example**
To associate VLAN classifier group 3 with switch 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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;vlan-class-group-id&gt;</code></td>
<td>Specify a VLAN classifier group identifier in the range &lt;1-16&gt;.</td>
</tr>
</tbody>
</table>
**VLAN COMMANDS**

**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**

```plaintext
vlan classifier group <1-16> {add|delete} rule <vlan-class-rule-id>
no vlan classifier group <1-16>
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-16&gt;</td>
<td>VLAN classifier group identifier</td>
</tr>
<tr>
<td>add</td>
<td>Add the rule to the group.</td>
</tr>
<tr>
<td>delete</td>
<td>Delete the rule from the group.</td>
</tr>
<tr>
<td>&lt;vlan-class-rule-id&gt;</td>
<td>The VLAN classifier rule identifier.</td>
</tr>
</tbody>
</table>

**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 COMMANDS
VLAN CLASSIFIER RULE IPV4

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>

Mode
Global Configuration

Usage
If the source IP address matches the IP subnet specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN.

Example
awplus# configure
terminal
awplus(config)# vlan classifier rule 3 ipv4 3.3.3.3/8 vlan 5

Related Commands
show vlan classifier rule
vlan classifier activate
vlan classifier rule proto

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-256&gt;</td>
<td>Specify the VLAN Classifier Rule identifier.</td>
</tr>
<tr>
<td>&lt;ip-addr/prefix-length&gt;</td>
<td>Specify the IP address and prefix length.</td>
</tr>
<tr>
<td>&lt;1-4094&gt;</td>
<td>Specify a VLAN ID to which an untagged packet is mapped in the range &lt;1-4094&gt;.</td>
</tr>
</tbody>
</table>
VLAN COMMANDS
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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-256&gt;</td>
<td>VLAN Classifier identifier</td>
</tr>
<tr>
<td>proto</td>
<td>Protocol type</td>
</tr>
<tr>
<td>&lt;protocol&gt;</td>
<td>Specify a protocol either by its decimal number (0-65535) or by one of the</td>
</tr>
<tr>
<td></td>
<td>following protocol names:</td>
</tr>
<tr>
<td>[arp</td>
<td>2054]</td>
</tr>
<tr>
<td>[atalkaarp</td>
<td>33011]</td>
</tr>
<tr>
<td>[atalkddp</td>
<td>32923]</td>
</tr>
<tr>
<td>[atmmulti</td>
<td>34892]</td>
</tr>
<tr>
<td>[atmtransport</td>
<td>34948]</td>
</tr>
<tr>
<td>[dec</td>
<td>24576]</td>
</tr>
<tr>
<td>[deccustom</td>
<td>24582]</td>
</tr>
<tr>
<td>[decdiagnostics</td>
<td>24581]</td>
</tr>
<tr>
<td>[decdnadumpload</td>
<td>24577]</td>
</tr>
<tr>
<td>[decnaremoteconsole</td>
<td>24578]</td>
</tr>
<tr>
<td>[decdnarouting</td>
<td>24579]</td>
</tr>
</tbody>
</table>
## VLAN CLASSIFIER RULE PROTO

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[declat</td>
<td>24580]</td>
</tr>
<tr>
<td>[decsyscomm</td>
<td>24583]</td>
</tr>
<tr>
<td>[g8bpqx25</td>
<td>2303]</td>
</tr>
<tr>
<td>[ieeeaddrtrans</td>
<td>2561]</td>
</tr>
<tr>
<td>[ieeepup</td>
<td>2560]</td>
</tr>
<tr>
<td>[ip</td>
<td>2048]</td>
</tr>
<tr>
<td>[ipv6</td>
<td>34525]</td>
</tr>
<tr>
<td>[ipx</td>
<td>33079]</td>
</tr>
<tr>
<td>[netbeui</td>
<td>61680]</td>
</tr>
<tr>
<td>[netbeui</td>
<td>61681]</td>
</tr>
<tr>
<td>[pppdiscovery</td>
<td>34915]</td>
</tr>
<tr>
<td>[pppsession</td>
<td>34916]</td>
</tr>
<tr>
<td>[rarp</td>
<td>32821]</td>
</tr>
<tr>
<td>[x25</td>
<td>2056]</td>
</tr>
<tr>
<td>[xeroxaddrtrans</td>
<td>513]</td>
</tr>
<tr>
<td>[xeroxpup</td>
<td>512]</td>
</tr>
<tr>
<td>ethv2</td>
<td>Ethernet Version 2 encapsulation</td>
</tr>
<tr>
<td>nosnapllc</td>
<td>LLC without SNAP encapsulation</td>
</tr>
<tr>
<td>snapllc</td>
<td>LLC SNAP encapsulation</td>
</tr>
<tr>
<td>&lt;1-4094&gt;</td>
<td>Specify a VLAN ID to which an untagged packet is mapped in the range &lt;1-4094&gt;</td>
</tr>
</tbody>
</table>

**Mode**: Global Configuration

**Usage**: If the protocol type matches the protocol specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN. Ethernet Frame Numbers may be entered in place of the protocol names listed. For a full list please refer to the IANA list online: [www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt](http://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt)
**Examples**

```
awplus# configure terminal
awplus(config)# vlan classifier rule 1 proto x25 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
awplus(config)# vlan classifier rule 5 proto encap ethv2 vlan 234525
awplus(config)# vlan classifier rule 6 proto encap ethv2 vlan 2ipv6
awplus(config)# vlan classifier rule 7 proto encap ethv2 vlan 22048
awplus(config)# vlan classifier rule 8 proto encap ethv2 vlan 2ip
```

**Validation**

```
awplus# show vlan classifier rule
```

<table>
<thead>
<tr>
<th>VLAN Classifier Rule</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan classifier rule 16 proto rarp encap ethv2 vlan 2</td>
<td></td>
</tr>
<tr>
<td>vlan classifier rule 8 proto encap ethv2 vlan 2</td>
<td></td>
</tr>
<tr>
<td>vlan classifier rule 4 proto arp encap ethv2 vlan 2</td>
<td></td>
</tr>
<tr>
<td>vlan classifier rule 3 proto xeroxpup encap ethv2 vlan 2</td>
<td></td>
</tr>
<tr>
<td>vlan classifier rule 2 proto ip encap ethv2 vlan 2</td>
<td></td>
</tr>
<tr>
<td>vlan classifier rule 1 proto ipv6 encap ethv2 vlan 2</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

- `show vlan classifier rule`
- `vlan classifier activate`
- `vlan classifier group`
### vlan database

**Overview**
Use this command to enter the VLAN Configuration mode.

**Syntax**
```
vlan database
```

**Mode**
Global Configuration

**Usage**
Use this command to enter the VLAN configuration mode. You can then add or delete a VLAN, or modify its values.

**Example**
In the following example, note the change to VLAN configuration mode from Configure mode:
```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)#
```

**Related Commands**
-vlan
VLAN COMMANDS
VLAN MODE STACK-LOCAL-VLAN

vlan mode stack-local-vlan

**Overview**  This command enables you to create stack-local-VLANs and use ICMP to monitor and diagnose issues within specific members of the stack. When a VLAN is added using this method, all its traffic will be trapped to and processed by the CPU of the specific local stack member, rather than the CPU of the stack master.

The **no** variant of this command destroys the specified VLAN.

**Syntax**  

```plaintext
vlan <vid> mode stack-local-vlan <member-id>
no vlan <vid>
```

**Parameter**  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| <vid>       | The VID of the VLAN to be created in the range 2-4094. We recommend that the first stack-local-vlan be assigned the number 4001 for the first stack member, then incremented by one for each stack member. So a stack of four members would be assigned the following VID numbers:  
stack member one VID 4001  
stack member two VID 4002  
stack member three VID 4003  
stack member four VID 4004 |
| mode stack-local-vlan | Specifies that the new VLAN will function as a stack-local-VLAN. |
| <member-id> | Specifies the new stack member ID. Enter a decimal number in the range 1-8. |

**Default**  By default, VLANs are automatically enabled as they are added.

**Mode**  VLAN Configuration

**Examples**  
To add a stack-local-VLAN with the VID of 4002 and assign it to stack member 2, use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 4002 mode stack-local-vlan
```

To remove VLAN 4002, use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 4002
```
VLAN COMMANDS
VLAN MODE STACK-LOCAL-VLAN

Related Commands

- mtu
- vlan database
- show vlan
VLAN COMMANDS
VLAN STATISTICS

VLAN STATISTICS

Overview
This command creates a VLAN packet counter instance, and enables you to add one or more ports to a defined counter instance. This command can only be applied to switch ports. You cannot apply it to aggregated links or eth ports.

The no variant of this command enables the deletion of VLAN packet counter instances, or for removing one or more ports that are currently mapped to a counter instance. Note that the selected range of ports must all be switch ports.

NOTE:
In describing this command, the terms frame and packet are used interchangeably.

Syntax
```
vlan <vid> statistics name <instance_name>
no vlan statistics name <instance_name>
```

Mode
Interface Configuration

Usage
A maximum of 128 packet counter instances can be created. When the first instance is configured, the switch will reserve sufficient resources to support 128 packet counter instances. These resources are also shared with other features such as QoS and ACLs. Where the remaining resources are insufficient to support the VLAN Statistics feature the feature will not be enabled, and an error message will display.

Examples
Create a VLAN packet counter instance named vlan2-data, and apply this to count incoming vlan2 tagged frames on ports 1.0.4 and 1.0.5.
```
awplus# configure terminal
awplus(config)# interface port1.0.4,port1.0.5
awplus(config-if)# vlan 2 statistics name vlan2-data
```

From the previous example, add ports in the range 1.0.2 to 1.0.3 to the VLAN packet counter instance. The vlan2-data instance will now count all incoming vlan2 tagged frames on ports within the range 1.0.1 to 1.0.5.
```
awplus(config)# interface port1.0.2-port1.0.3
awplus(config-if)# vlan 2 statistics name vlan2-data
```

To remove port1.0.5 from the packet counter instance named vlan2-data.
```
awplus(config)# interface port1.0.5
awplus(config-if)# no vlan statistics name vlan2-data
```
To remove the remaining ports 1.0.2 to 1.0.4 from the packet counter instance named **vlan2-data**. Note that because there are no ports associated with the **vlan2-data**, this instance will be removed.

```
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# no vlan statistics name vlan2-data
```

**Related Commands**

- clear vlan statistics
- show vlan statistics
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 496
- “clear spanning-tree detected protocols (RSTP and MSTP)” on page 497
- “debug mstp (RSTP and STP)” on page 498
- “instance priority (MSTP)” on page 502
- “instance vlan (MSTP)” on page 504
- “region (MSTP)” on page 506
- “revision (MSTP)” on page 507
- “show debugging mstp” on page 508
- “show spanning-tree” on page 509
- “show spanning-tree brief” on page 512
- “show spanning-tree mst” on page 513
- “show spanning-tree mst config” on page 514
- “show spanning-tree mst detail” on page 515
- “show spanning-tree mst detail interface” on page 517
- “show spanning-tree mst instance” on page 519
- “show spanning-tree mst instance interface” on page 520
- “show spanning-tree mst interface” on page 521
- “show spanning-tree mst detail interface” on page 522
- “show spanning-tree statistics” on page 524
- “show spanning-tree statistics instance” on page 526
- “show spanning-tree statistics instance interface” on page 528
- “show spanning-tree statistics interface” on page 530
- “show spanning-tree vlan range-index” on page 534
- “spanning-tree autoedge (RSTP and MSTP)” on page 535
- “spanning-tree bpdu” on page 536
- “spanning-tree cisco-interoperability (MSTP)” on page 538
- “spanning-tree edgeport (RSTP and MSTP)” on page 539
- “spanning-tree enable” on page 540
- “spanning-tree errdisable-timeout enable” on page 542
- “spanning-tree errdisable-timeout interval” on page 543
- “spanning-tree force-version” on page 544
- “spanning-tree forward-time” on page 545
- “spanning-tree guard root” on page 546
- “spanning-tree hello-time” on page 547
- “spanning-tree link-type” on page 548
SPANNING TREE COMMANDS

- “spanning-tree max-age” on page 549
- “spanning-tree max-hops (MSTP)” on page 550
- “spanning-tree mode” on page 551
- “spanning-tree mst configuration” on page 552
- “spanning-tree mst instance” on page 553
- “spanning-tree mst instance path-cost” on page 554
- “spanning-tree mst instance priority” on page 556
- “spanning-tree mst instance restricted-role” on page 557
- “spanning-tree mst instance restricted-tcn” on page 558
- “spanning-tree path-cost” on page 560
- “spanning-tree portfast (STP)” on page 561
- “spanning-tree portfast bpdu-filter” on page 563
- “spanning-tree portfast bpdu-guard” on page 565
- “spanning-tree priority (bridge priority)” on page 567
- “spanning-tree priority (port priority)” on page 568
- “spanning-tree restricted-role” on page 569
- “spanning-tree restricted-tcn” on page 570
- “spanning-tree transmit-holdcount” on page 571
- “undebug mstp” on page 572
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>]]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>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).</td>
</tr>
<tr>
<td>&lt;mstp-instance&gt;</td>
<td>The MSTP instance (MSTI - Multiple Spanning Tree Instance) to clear MSTP BPDU statistics.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Usage**
Use this command with the `instance` parameter in MSTP mode. Specifying this command with the `interface` parameter only not the instance parameter will work in STP and RSTP mode.

**Examples**
```
awplus# clear spanning-tree statistics
awplus# clear spanning-tree statistics instance 1
awplus# clear spanning-tree statistics interface port1.0.2
awplus# clear spanning-tree statistics interface port1.0.2 instance 1
```
clear spanning-tree detected protocols (RSTP and MSTP)

**Overview**
Use this command to clear the detected protocols for a specific port, or all ports. Use this command in RSTP or MSTP mode only.

**Syntax**
clear spanning-tree detected protocols [interface <port>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>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).</td>
</tr>
</tbody>
</table>

**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 as 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>]}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Echoes all spanning tree debugging levels to the console.</td>
</tr>
<tr>
<td>cli</td>
<td>Echoes spanning tree commands to the console.</td>
</tr>
<tr>
<td>packet</td>
<td>Echoes spanning tree packets to the console.</td>
</tr>
<tr>
<td>rx</td>
<td>Received packets.</td>
</tr>
<tr>
<td>tx</td>
<td>Transmitted packets.</td>
</tr>
<tr>
<td>protocol</td>
<td>Echoes protocol changes to the console.</td>
</tr>
<tr>
<td>timer</td>
<td>Echoes timer information to the console.</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed output.</td>
</tr>
<tr>
<td>decode</td>
<td>Interprets packet contents</td>
</tr>
<tr>
<td>topology-change</td>
<td>Interprets topology change messages</td>
</tr>
<tr>
<td>interface</td>
<td>Keyword before &lt;interface&gt; placeholder to specify an interface to debug</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>Placeholder used to specify the name of the interface to debug</td>
</tr>
</tbody>
</table>

**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:
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
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 : 3ab68794d602f3d43b21c0b37ac3bca8
17:23:42 awplus MSTP[1417]: CIST bridge id : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST int pathcost : 0
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
```
SPANNING TREE COMMANDS
DEBUG MSTP (RSTP AND STP)

**Examples**

```plaintext
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
- unddebug mstp
**instance priority (MSTP)**

**Overview**
Use this command to set the priority for this device to become the root bridge for the specified MSTI (Multiple Spanning Tree Instance).

Use this command for MSTP only.

Use the `no` variant of this command to restore the root bridge priority of the device for the instance to the default.

**Syntax**
```
instance <msti-id> priority <priority>
no instance <msti-id> priority
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;msti-id&gt;</code></td>
<td>Specify the MST instance ID in the range <code>&lt;1-15&gt;</code>.</td>
</tr>
<tr>
<td><code>&lt;priority&gt;</code></td>
<td>Specify the root bridge priority for the device for the MSTI in the range <code>&lt;0-61440&gt;</code>. 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.</td>
</tr>
</tbody>
</table>

**Default**
The default priority value for all instances is 32768.

**Mode**
MST Configuration

**Usage**
MSTP lets you distribute traffic more efficiently across a network by blocking different links for different VLANs. You do this by making different devices into the root bridge for each MSTP instance, so that each instance blocks a different link.

If all devices have the same root bridge priority for the instance, MSTP selects the device with the lowest MAC address to be the root bridge. Give the device a higher priority for becoming the root bridge for a particular instance by assigning it a lower priority number, or vice versa.

**Examples**
To set the root bridge priority for MSTP instance 2 to be the highest (0), so that it will be the root bridge for this instance when available, use the commands:
```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 2 priority 0
```

To reset the root bridge priority for instance 2 to the default (32768), use the commands:
```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# no instance 2 priority
```
Related Commands
region (MSTP)
revision (MSTP)
show spanning-tree mst config
spanning-tree mst instance
spanning-tree mst instance priority
instance vlan (MSTP)

Overview
Use this command to create an MST Instance (MSTI), and associate the specified VLANs with it. An MSTI is a spanning tree instance that exists within an MST region (MSTR). An MSTR can contain up to 15 MSTIs.

When a VLAN is associated with an MSTI the member ports of the VLAN are automatically configured to send and receive spanning-tree information for the associated MSTI. You can disable this automatic configuration of member ports of the VLAN to the associated MSTI by using a `no spanning-tree mst instance` command to remove the member port from the MSTI.

Use the `instance vlan` command for MSTP only.

Use the `no` variant of this command to remove the specified VLANs from the MSTI.

Syntax
```
instance <msti-id> vlan {<vid>|<vid-list>}
nor instance <msti-id> vlan {<vid>|<vid-list>}
```

Mode
MST Configuration

Usage
The VLANs must be created before being associated with an MST instance (MSTI). If the VLAN range is not specified, the MSTI will not be created.

This command removes the specified VLANs from the CIST and adds them to the specified MSTI. If you use the `no` variant of this command to remove the VLAN from the MSTI, it returns it to the CIST. To move a VLAN from one MSTI to another, you must first use the `no` variant of this command to return it to the CIST.

Ports in these VLANs will remain in the control of the CIST until you associate the ports with the MSTI using the `spanning-tree mst instance` command.

Example
```
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 2 vlan 30
```
Related Commands

- region (MSTP)
- revision (MSTP)
- show spanning-tree mst config
- spanning-tree mst instance
- vlan
region (MSTP)

**Overview**
Use this command to assign a name to the device's MST Region. MST Instances (MSTI) of a region form different spanning trees for different VLANs.

Use this command for MSTP only.

Use the `no` variant of this command to remove this region name and reset it to the default.

**Syntax**
```
region <region-name>
no region
```

**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>
```

**Default**
The default of revision number is 0.

**Mode**
MST Configuration

**Usage**
The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

**Example**
```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# revision 25
```

**Related Commands**
- `region (MSTP)`
- `show spanning-tree mst config`
- `instance vlan (MSTP)`
**show debugging mstp**

**Overview** Use this command to show the MSTP debugging options set. For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax** show debugging mstp

**Mode** User Exec and Privileged Exec mode

**Example** To display the MSTP debugging options set, enter the command:

```
awplus# show debugging mstp
```

**Output** Figure 12-1: Example output from the `show debugging mstp` command

```
MSTP debugging status:
  MSTP receiving packet debugging is on
```

**Related Commands** `debug mstp` (RSTP and STP)
show spanning-tree

**Overview**
Use this command to display detailed spanning tree information on the specified port or on all ports. Use this command for RSTP, MSTP or STP.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show spanning-tree [interface <port-list>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Display information about the following port only.</td>
</tr>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports to display information about. A port-list can be:</td>
</tr>
<tr>
<td></td>
<td>- a switch port (e.g. port1.0.6) a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</td>
</tr>
<tr>
<td></td>
<td>- a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.4, or sa1-2, or po1-2</td>
</tr>
<tr>
<td></td>
<td>- 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</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Usage**
Note that any list of interfaces specified must not span any interfaces that are not installed.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the `show spanning-tree` command. You can see the topology change counter for MSTP by using the `show spanning-tree mst instance` command.

**Example**
To display spanning tree information about port1.0.3, use the command:
```
awplus# show spanning-tree interface port1.0.3
```
**Output** Figure 12-2: Example output from the `show spanning-tree` command

```
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000000cd20f093
% 1: Bridge Id 80000000cd20f093
% 1: last topology change Sun Nov 20 12:24:24 1977
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.3: Port 5023 - Id 839f - Role Designated - State Forwarding
%   port1.0.3: Designated Path Cost 0
%   port1.0.3: Configured Path Cost 200000 - Add type Explicit ref count 1
%   port1.0.3: Designated Port Id 839f - Priority 128 -
%   port1.0.3: Root 80000000cd20f093
%   port1.0.3: Designated Bridge 80000000cd20f093
%   port1.0.3: Message Age 0 - Max Age 20
%   port1.0.3: Hello Time 2 - Forward Delay 15
%   port1.0.3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   port1.0.3: forward-transitions 32
%   port1.0.3: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   port1.0.3: No portfast configured - Current portfast off
%   port1.0.3: portfast bpdu-guard default - Current portfast bpdu-guard off
%   port1.0.3: portfast bpdu-filter default - Current portfast bpdu-filter off
%   port1.0.3: no root guard configured - Current root guard off
%   port1.0.3: Configured Link Type point-to-point - Current point-to-point
```

Figure 12-3: Example output from the `show spanning-tree` command in RSTP mode
### SPANNING TREE COMMANDS

#### SHOW SPANNING-TREE

```
awplus#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000000cd24ff2d
% 1: Bridge Id 80000000cd24ff2d
% 1: last topology change Thu Jul 26 02:06:26 2007
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% port1.0.1: Port 5001 - Id 8389 - Role Disabled - State Discarding
% port1.0.1: Designated Path Cost 0
% port1.0.1: Configured Path Cost 20000000 - Add type Explicit ref count 1
% port1.0.1: Designated Port Id 8389 - Priority 128 -
% port1.0.1: Root 80000000cd24ff2d
% port1.0.1: Designated Bridge 80000000cd24ff2d
% port1.0.1: Message Age 0 - Max Age 20
% port1.0.1: Hello Time 2 - Forward Delay 15
% port1.0.1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
% port1.0.1: forward-transitions 0
% port1.0.1: Version Rapid Spanning Tree Protocol - Received None - Send STP
% port1.0.1: portfast configured - Current portfast off
% port1.0.1: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.1: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.1: no root guard configured - Current root guard off
% port1.0.1: Configured Link Type point-to-point - Current shared
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated Path Cost 0
% port1.0.2: Configured Path Cost 20000000 - Add type Explicit ref count 1
% port1.0.2: Designated Port Id 838a - Priority 128 -
% port1.0.2: Root 80000000cd24ff2d
% port1.0.2: Designated Bridge 80000000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 20
% port1.0.2: Hello Time 2 - Forward Delay 15
% port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
% port1.0.2: forward-transitions 0
% port1.0.2: Version Rapid Spanning Tree Protocol - Received None - Send STP
% port1.0.2: No portfast configured - Current portfast off
% port1.0.2: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.2: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.2: no root guard configured - Current root guard off
% port1.0.2: Configured Link Type point-to-point - Current shared
```
show spanning-tree brief

**Overview** Use this command to display a summary of spanning tree status information on all ports. Use this command for RSTP, MSTP or STP.

**Syntax**
```
show spanning-tree brief
```

**Mode** User Exec and Privileged Exec

**Usage** Note that any list of interfaces specified must not span any interfaces that are not installed.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the `show spanning-tree` command. You can see the topology change counter for MSTP by using the `show spanning-tree mst instance` command.

**Example** To display a summary of spanning tree status information, use the command:
```
awplus# show spanning-tree brief
```

**Output** Figure 12-4: Example output from the `show spanning-tree brief` command

```
Default: Bridge up - Spanning Tree Enabled
Default: Root Path Cost 40000 - Root Port 4501 - Bridge Priority 32768
Default: Root Id 8000:0000cd250001
Default: Bridge Id 8000:0000cd296eb1

<table>
<thead>
<tr>
<th>Port</th>
<th>Designated Bridge</th>
<th>Port Id</th>
<th>Role</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>sa1</td>
<td>8000:001577c9744b</td>
<td>8195</td>
<td>Rootport</td>
<td>Forwarding</td>
</tr>
<tr>
<td>po1</td>
<td>8000:0000cd296eb1</td>
<td>81f9</td>
<td>Designated</td>
<td>Forwarding</td>
</tr>
<tr>
<td>port1.0.1</td>
<td>8000:0000cd296eb1</td>
<td>8389</td>
<td>Disabled</td>
<td>Discarding</td>
</tr>
<tr>
<td>port1.0.2</td>
<td>8000:0000cd296eb1</td>
<td>838a</td>
<td>Disabled</td>
<td>Discarding</td>
</tr>
<tr>
<td>port1.0.3</td>
<td>8000:0000cd296eb1</td>
<td>838b</td>
<td>Disabled</td>
<td>Discarding</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>8000:0000cd296eb1</td>
<td>838c</td>
<td>Disabled</td>
<td>Discarding</td>
</tr>
<tr>
<td>port1.0.5</td>
<td>8000:0000cd296eb1</td>
<td>838d</td>
<td>Disabled</td>
<td>Discarding</td>
</tr>
<tr>
<td>port1.0.6</td>
<td>8000:0000cd296eb1</td>
<td>838e</td>
<td>Disabled</td>
<td>Discarding</td>
</tr>
</tbody>
</table>
```

**Related Commands** `show spanning-tree`
**show spanning-tree mst**

**Overview**
This command displays bridge-level information about the CIST and VLAN to MSTI mappings.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
show spanning-tree mst

**Mode**
User Exec, Privileged Exec and Interface Configuration

**Example**
To display bridge-level information about the CIST and VLAN to MSTI mappings, enter the command:

```
awplus# show spanning-tree mst
```

**Output**
Figure 12-5: Example output from the **show spanning-tree mst** command

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000000475e93ffe
% 1: 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
```
show spanning-tree mst config

Overview  Use this command to display MSTP configuration identifier for the device.

Syntax    show spanning-tree mst config

Mode      User Exec, Privileged Exec and Interface Configuration

Usage     The region name, the revision number, and the digest of the VLAN to MSTI
           configuration table must be the same on all devices that are intended to be in the
           same MST region.

Example   To display MSTP configuration identifier information, enter the command:
           awplus# show spanning-tree mst config

Output    Figure 12-6: Example output from the show spanning-tree mst config
           command

           awplus#show spanning-tree mst config
           %
           % MSTP Configuration Information:
           %------------------------------------------------------
           % Format Id    : 0
           % Name         : My Name
           % Revision Level : 0
           % Digest       : 0x80DEE46DA92A98CF21C603291B22880A
           %------------------------------------------------------

Related Commands
instance vlan (MSTP)
region (MSTP)
revision (MSTP)
**show spanning-tree mst detail**

**Overview**  
This command displays detailed information about each instance, and all interfaces associated with that particular instance.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
`show spanning-tree mst detail`

**Mode**  
User Exec, Privileged Exec and Interface Configuration

**Example**  
To display detailed information about each instance, and all interfaces associated with them, enter the command:

```
awplus# show spanning-tree mst detail
```

**Output**  
Figure 12-7: Example output from the `show spanning-tree mst detail` command
SPANNING TREE COMMANDS
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 Req Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% port1.0.1: Port 5001 - Id 8389 - Role Disabled - State Discarding
% port1.0.1: Designated External Path Cost 0 - Internal Path Cost 0
% port1.0.1: Configured Path Cost 20000000 - Add type Explicit ref count 1
% port1.0.1: Designated Port Id 8389 - CIST Priority 128 -
% port1.0.1: CIST Root 80000000cd24ff2d
% port1.0.1: Regional Root 80000000cd24ff2d
% port1.0.1: Designated Bridge 80000000cd24ff2d
% port1.0.1: Message Age 0 - Max Age 20
% port1.0.1: CIST Hello Time 2 - Forward Delay 15
% port1.0.1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
% .
% port1.0.2: forward-transitions 0
% port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
% port1.0.2: No portfast configured - Current portfast off
% port1.0.2: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.2: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.2: no root guard configured - Current root guard off
% port1.0.2: Configured Link Type point-to-point - Current shared
% port1.0.3: Port 5003 - Id 838b - Role Disabled - State Discarding
% port1.0.3: Designated External Path Cost 0 - Internal Path Cost 0
% port1.0.3: Configured Path Cost 20000000 - Add type Explicit ref count 1
% port1.0.3: Designated Port Id 838b - CIST Priority 128 -
% port1.0.3: CIST Root 80000000cd24ff2d
% port1.0.3: Regional Root 80000000cd24ff2d
% port1.0.3: Designated Bridge 80000000cd24ff2d
% port1.0.3: Message Age 0 - Max Age 20
% port1.0.3: CIST Hello Time 2 - Forward Delay 15
% port1.0.3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
% port1.0.3: forward-transitions 0
% port1.0.3: Version Multiple Spanning Tree Protocol - Received None - Send STP
% port1.0.3: No portfast configured - Current portfast off
% port1.0.3: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.3: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.3: no root guard configured - Current root guard off
% port1.0.3: Configured Link Type point-to-point - Current shared
show spanning-tree mst detail interface

**Overview**
This command displays detailed information about the specified switch port, and the MST instances associated with it.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```plaintext
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:
```plaintext
awplus# show spanning-tree mst detail interface port1.0.3
```

**Output**
Figure 12-8: Example output from the `show spanning-tree mst detail interface` command
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: Portfast bpdu-filter disabled
% 1: Portfast bpdu-guard disabled
% 1: Portfast errdisable timeout disabled
% 1: Portfast errdisable timeout interval 300 sec
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated External Path Cost 0 - Internal Path Cost 0
% port1.0.2: Configured Path Cost 20000000 - Add type Explicit ref count 2
% port1.0.2: Designated Port Id 838a - CIST Priority 128 -
% port1.0.2: CIST Root 80000000cd24ff2d
% port1.0.2: Regional Root 80000000cd24ff2d
% port1.0.2: Designated Bridge 80000000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 20
% port1.0.2: CIST Hello Time 2 - Forward Delay 15
% port1.0.2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
% port1.0.2: forward-transitions 0
% port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
% port1.0.2: No portfast configured - Current portfast off
% port1.0.2: Portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.2: Portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.2: No root guard configured - Current root guard off
% port1.0.2: Configured Link Type point-to-point - Current shared
% Instance 2: Vlans: 2
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated Internal Path Cost 0 - Designated Port Id 838a
% port1.0.2: Configured Internal Path Cost 20000000
% port1.0.2: Configured CST External Path cost 20000000
% port1.0.2: CST Priority 128 - MSTI Priority 128
% port1.0.2: Designated Root 80020000cd24ff2d
% port1.0.2: Designated Bridge 80020000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 0
% port1.0.2: Hello Time 2 - Forward Delay 15
% port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
show spanning-tree mst instance

Overview  This command displays detailed information for the specified instance, and all
switch ports associated with that instance.

A topology change counter has been included for RSTP and MSTP. You can see the
topology change counter for RSTP by using the show spanning-tree command.
You can see the topology change counter for MSTP by using the show
spanning-tree mst instance command.

For information on filtering and saving command output, see “Controlling “show”
Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview
and Configuration Guide.

Syntax  show spanning-tree mst instance <instance>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;instance&gt;</td>
<td>Specify an MSTP instance in the range &lt;1-15&gt;.</td>
</tr>
</tbody>
</table>

Mode  User Exec, Privileged Exec, and Interface Configuration

Usage  To display detailed information for instance 2, and all switch ports associated with
that instance, use the command:

awplus# show spanning-tree mst instance 2

Output  Figure 12-9: Example output from the show spanning-tree mst instance
command

% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated Internal Path Cost 0 - Designated Port Id 838a
% port1.0.2: Configured Internal Path Cost 20000000
% port1.0.2: Configured CST External Path cost 20000000
% port1.0.2: CST Priority 128 - MSTI Priority 128
% port1.0.2: Designated Root 80020000cd24ff2d
% port1.0.2: Designated Bridge 80020000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 0
% port1.0.2: Hello Time 2 - Forward Delay 15
% port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
show spanning-tree mst instance interface

**Overview**
This command displays detailed information for the specified MST (Multiple Spanning Tree) instance, and the specified switch port associated with that MST instance.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
`show spanning-tree mst instance <instance> interface <port>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;instance&gt;</code></td>
<td>Specify an MSTP instance in the range &lt;1-15&gt;.</td>
</tr>
<tr>
<td><code>&lt;port&gt;</code></td>
<td>The port to display information about. The port may be a switch port (e.g. <code>port1.0.4</code>), a static channel group (e.g. <code>sa2</code>), or a dynamic (LACP) channel group (e.g. <code>po2</code>).</td>
</tr>
</tbody>
</table>

**Mode**
User Exec, Privileged Exec, and Interface Configuration

**Example**
To display detailed information for instance 2, interface `port1.0.2`, use the command:

`awplus# show spanning-tree mst instance 2 interface port1.0.2`

**Output**
Figure 12-10: Example output from the `show spanning-tree mst instance` command

```plaintext
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated Internal Path Cost 0 - Designated Port Id 838a
% port1.0.2: Configured Internal Path Cost 20000000
% port1.0.2: Configured CST External Path cost 20000000
% port1.0.2: CST Priority 128  - MSTI Priority 128
% port1.0.2: Designated Root 80020000cd24ff2d
% port1.0.2: Designated Bridge 80020000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 0
% port1.0.2: Hello Time 2 - Forward Delay 15
% port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```
show spanning-tree mst interface

**Overview**  This command displays the number of instances created, and VLANs associated with it for the specified switch port.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show spanning-tree mst interface <port>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>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).</td>
</tr>
</tbody>
</table>

**Mode**  User Exec, Privileged Exec, and Interface Configuration

**Example**  To display detailed information about each instance, and all interfaces associated with them, for port1.0.4, use the command:

```
awplus# show spanning-tree mst interface port1.0.4
```

**Output**  Figure 12-11: Example output from the `show spanning-tree mst interface` command

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000008c73a2b22
% 1: CIST Reg Root Id 80000008c73a2b22
% 1: CST Bridge Id 80000008c73a2b22
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
% 1: 
% Instance      VLAN
% 0:             1
% 1:             2-3
% 2:             4-5
```
show spanning-tree mst detail interface

**Overview**
This command displays detailed information about the specified switch port, and the MST instances associated with it.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
show spanning-tree mst detail interface <port>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>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).</td>
</tr>
</tbody>
</table>

**Mode**
User Exec, Privileged Exec and Interface Configuration

**Example**
To display detailed information about port1.0.3 and the instances associated with it, enter the command:

```
awplus# show spanning-tree mst detail interface port1.0.3
```

**Output**
Figure 12-12: Example output from the show spanning-tree mst detail interface command
```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Root Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated External Path Cost 0 - Internal Path Cost 0
% port1.0.2: Configured Path Cost 20000000 - Add type Explicit ref count 2
% port1.0.2: Designated Port Id 838a - CIST Priority 128 -
% port1.0.2: CIST Root 80000000cd24ff2d
% port1.0.2: Regional Root 80000000cd24ff2d
% port1.0.2: Designated Bridge 80000000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 20
% port1.0.2: CIST Hello Time 2 - Forward Delay 15
% port1.0.2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
% change timer 0
% port1.0.2: forward-transitions 0
% port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
% port1.0.2: no portfast configured - Current portfast off
% port1.0.2: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.2: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.2: no root guard configured - Current root guard off
% port1.0.2: Configured Link Type point-to-point - Current shared
% Instance 2: Vlans: 2
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated Internal Path Cost 0 - Designated Port Id 838a
% port1.0.2: Configured Internal Path Cost 20000000
% port1.0.2: Configured CST External Path cost 20000000
% port1.0.2: CST Priority 128 - MSTI Priority 128
% port1.0.2: Designated Root 80020000cd24ff2d
% port1.0.2: Designated Bridge 80020000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 0
% port1.0.2: Hello Time 2 - Forward Delay 15
% port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```
show spanning-tree statistics

**Overview**
This command displays BPDU (Bridge Protocol Data Unit) statistics for all spanning-tree instances, and all switch ports associated with all spanning-tree instances.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show spanning-tree statistics
```

**Mode**
Privileged Exec

**Usage**
To display BPDU statistics for all spanning-tree instances, and all switch ports associated with all spanning-tree instances, use the command:
```
awplus# show spanning-tree statistics
```

**Output**
Figure 12-13: Example output from the `show spanning-tree statistics` command
### SPANNING TREE COMMANDS

#### SHOW SPANNING-TREE STATISTICS

<table>
<thead>
<tr>
<th>Port number</th>
<th>Interface</th>
<th>--------------------</th>
<th>-----------------</th>
<th>-----------------------------</th>
<th>---</th>
<th>---</th>
<th>---</th>
<th>---</th>
</tr>
</thead>
<tbody>
<tr>
<td>915</td>
<td>port1.0.6</td>
<td>% BPDU Related Parameters</td>
<td>% Port Spanning Tree</td>
<td>Disable</td>
<td>% Spanning Tree Type</td>
<td>Rapid Spanning Tree Protocol</td>
<td>% Current Port State</td>
<td>Discarding</td>
</tr>
</tbody>
</table>
|             |                 | % 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 | % Forward Delay Timer | INACTIVE | % Forward Delay Timer Value | 0 | % Message Age Timer | INACTIVE | % Message Age Timer Value | 0 | % Topology Change Timer | INACTIVE | % Topology Change Timer Value | 0 | % Hold Timer | INACTIVE | % Hold Timer Value | 0 | % Other Port-Specific Info | % Max Age Transitions | 1 | % Msg Age Expiry | 0 | % Similar BPDUS Rcvd | 0 | % Src Mac Count | 0 | % Total Src Mac Rcvd | 0 | % Next State | Learning | % Topology Change Time | 0 |
show spanning-tree statistics instance

**Overview**  
This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST (Multiple Spanning Tree) instance, and all switch ports associated with that MST instance.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
`show spanning-tree statistics instance <instance>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `<instance>` | Specify an MSTP instance in the range `<1-15>`.

**Mode**  
Privileged Exec

**Usage**  
To display BPDU statistics information for MST instance 2, and all switch ports associated with that MST instance, use the command:

`awplus# show spanning-tree statistics instance 2`
Output

Figure 12-14: Example output from the `show spanning-tree statistics instance` command:

```
% % INST_PORT port1.0.3 Information & Statistics
% ----------------------------------------
% Config Bpdu's transmitted (port/inst) : (0/0)
% Config Bpdu's received (port/inst)    : (0/0)
% TCN Bpdu's transmitted (port/inst)    : (0/0)
% TCN Bpdu's received (port/inst)      : (0/0)
% Message Age (port/Inst)              : (0/0)
% port1.0.3: Forward Transitions       : 0
% Next State                           : Learning
% Topology Change Time                 : 0
% INST_PORT port1.0.4 Information & Statistics
% ----------------------------------------
% Config Bpdu's transmitted (port/inst) : (0/0)
% Config Bpdu's received (port/inst)    : (0/0)
% TCN Bpdu's transmitted (port/inst)    : (0/0)
% TCN Bpdu's received (port/inst)      : (0/0)
% Message Age (port/Inst)              : (0/0)
% port1.0.4: Forward Transitions       : 0
% Next State                           : Learning
% Topology Change Time                 : 0
% INST_PORT port1.0.5 Information & Statistics
% ----------------------------------------
% Config Bpdu's transmitted (port/inst) : (0/0)
% Config Bpdu's received (port/inst)    : (0/0)
% TCN Bpdu's transmitted (port/inst)    : (0/0)
% TCN Bpdu's received (port/inst)      : (0/0)
% Message Age (port/Inst)              : (0/0)
% port1.0.5: Forward Transitions       : 0
% Next State                           : Learning
% Topology Change Time                 : 0
```
show spanning-tree statistics instance interface

**Overview**
This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST (Multiple Spanning Tree) instance and the specified switch port associated with that MST instance.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
show spanning-tree statistics instance <instance> interface <port>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;instance&gt;</td>
<td>Specify an MSTP instance in the range &lt;1-15&gt;.</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td>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).</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
To display BPDU statistics for MST instance 2, interface port1.0.2, use the command:

```
awplus# show spanning-tree statistics instance 2 interface port1.0.2
```
**Output**  Figure 12-15: Example output from the `show spanning-tree statistics instance interface` command

```
awplus#sh spanning-tree statistics interface port1.0.2 instance 1
  Spanning Tree Enabled for Instance : 1
  % INST_PORT port1.0.2 Information & Statistics
  % ----------------------------------------
  % Config Bpdu's xmitted (port/inst)    : (0/0)
  % Config Bpdu's received (port/inst)   : (0/0)
  % TCN Bpdu's xmitted (port/inst)       : (0/0)
  % TCN Bpdu's received (port/inst)      : (0/0)
  % Message Age(port/Inst)               : (0/0)
  % port1.0.2: Forward Transitions       : 0
  % Next State                           : Learning
  % Topology Change Time                 : 0
  % Other Inst/Vlan Information & Statistics
  % ----------------------------------------
  % Bridge Priority                     : 0
  % Bridge Mac Address                   : ec:cd:6d:20:c0:ed
  % Topology Change Initiator           : 5023
  % Last Topology Change Occured         : Mon Aug 22 05:42:06 2011
  % Topology Change                     : FALSE
  % Topology Change Detected             : FALSE
  % Topology Change Count                : 1
  % Topology Change Last Recvd from      : 00:00:00:00:00:00
```
show spanning-tree statistics interface

**Overview**
This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified switch port, and all MST instances associated with that switch port.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show spanning-tree statistics interface <port>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>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).</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
To display BPDU statistics about each MST instance for port1.0.4, use the command:

```
awplus# show spanning-tree statistics interface port1.0.4
```
Output  Figure 12-16: Example output from the **show spanning-tree statistics interface** command
awplus#show
spanning-tree statistics interface port1.0.2

Port number = 906 Interface = port1.0.2

% BPDU Related Parameters
% -----------------------
% Port Spanning Tree : Disable
% Spanning Tree Type : Multiple Spanning Tree Protocol
% Current Port State : Discarding
% Port ID : 838a
% Port Number : 38a
% Path Cost : 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 Aug 22 05:41:20 2011
% Topology Change : FALSE
% Topology Change Detected : TRUE
% Topology Change Count : 1
SPANNING TREE COMMANDS
SHOW SPANNING-TREE STATISTICS INTERFACES

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 12-17: Example output from the `show spanning-tree vlan range-index` command

```
awplus#show spanning-tree vlan range-index
% MST Instance  VLAN       RangeIdx
%     1        1          1
%
```

**Related Commands**
show spanning-tree statistics
spanning-tree autoedge (RSTP and MSTP)

**Overview**

Use this command to enable the autoedge feature on the port.

The autoedge feature allows the port to automatically detect that it is an edge port. If it does not receive any BPDUs in the first three seconds after linkup, enabling, or entering RSTP or MSTP mode, it sets itself to be an edgeport and enters the forwarding state.

Use this command for RSTP or MSTP.

Use the `no` variant of this command to disable this feature.

**Syntax**

```
spanning-tree autoedge

no spanning-tree autoedge
```

**Default**

Disabled

**Mode**

Interface Configuration

**Example**

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# spanning-tree autoedge
```

**Related Commands**

spanning-tree edgeport (RSTP and MSTP)
spanning-tree bpdu

**Overview**
Use this command in Global Configuration mode to configure BPDU (Bridge Protocol Data Unit) discarding or forwarding, with STP (Spanning Tree Protocol) disabled on the switch.

See the Usage note about disabling Spanning Tree before using this command, and using this command to forward unsupported BPDUs unchanged for unsupported STP Protocols.

There is not a no variant for this command. Instead, apply the discard parameter to reset it back to the default then re-enable STP with spanning-tree enable command.

**Syntax**
```
spanning-tree bpdu
(discard|forward|forward-untagged-vlan|forward-vlan)
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpdu</td>
<td>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):</td>
</tr>
<tr>
<td>discard</td>
<td>Discards all ingress STP BPDU frames.</td>
</tr>
<tr>
<td>forward</td>
<td>Forwards any ingress STP BPDU packets to all ports, regardless of any VLAN membership.</td>
</tr>
<tr>
<td>forward-untagged-vlan</td>
<td>Forwards any ingress STP BPDU frames to all ports that are untagged members of the ingress port's native VLAN.</td>
</tr>
<tr>
<td>forward-vlan</td>
<td>Forwards any ingress STP BPDU frames to all ports that are tagged members of the ingress port's native VLAN.</td>
</tr>
</tbody>
</table>

**Default**
The discard parameter is enabled by default.

**Mode**
Global Configuration

**Usage**
You must first disable Spanning Tree with the spanning-tree enable command before you can use this command to then configure BPDU discarding or forwarding.

This command enables the switch to forward unsupported BPDUs with an unsupported Spanning Tree Protocol, such as proprietary STP protocols with unsupported BPDUs, by forwarding BDPU (Bridge Protocol Data Unit) frames unchanged through the switch.

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 enable command.
Examples

To enable STP BPDU discard in Global Configuration mode with STP disabled, which discards all ingress STP BPDU frames, enter the commands:

awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu discard

To enable STP BPDU forward in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports regardless of any VLAN membership, enter the commands:

awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward

To enable STP BPDU forwarding for untagged frames in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports that are untagged members of the ingress port’s native VLAN, enter the commands:

awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward-untagged-vlan

To enable STP BPDU forwarding for tagged frames in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports that are tagged members of the ingress port’s native VLAN, enter the commands:

awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward-vlan

To reset STP BPDU back to the default discard parameter and re-enable STP on the switch, enter the commands:

awplus# configure terminal
awplus(config)# spanning-tree bpdu discard
awplus(config)# spanning-tree stp enable

Related Commands

show spanning-tree
spanning-tree enable
spanning-tree cisco-interoperability (MSTP)

Overview
Use this command to enable/disable Cisco-interoperability for MSTP.
Use this command for MSTP only.

Syntax
spanning-tree cisco-interoperability {enable|disable}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable Cisco interoperability for MSTP.</td>
</tr>
<tr>
<td>disable</td>
<td>Disable Cisco interoperability for MSTP.</td>
</tr>
</tbody>
</table>

Default
If this command is not used, Cisco interoperability is disabled.

Mode
Global Configuration

Usage
For compatibility with certain Cisco devices, all devices in the switched LAN running the AlliedWare Plus™ Operating System must have Cisco-interoperability enabled. When the AlliedWare Plus Operating System is interoperating with Cisco, the only criteria used to classify a region are the region name and revision level. VLAN to instance mapping is not used to classify regions when interoperating with Cisco.

Examples
To enable Cisco interoperability on a Layer 2 device:

```
awplus# configure terminal
awplus(config)# spanning-tree cisco-interoperability enable
```

To disable Cisco interoperability on a Layer 2 device:

```
awplus# configure terminal
awplus(config)# spanning-tree cisco-interoperability disable
```
**spanning-tree edgeport (RSTP and MSTP)**

**Overview**
Use this command to set a port as an edge-port.

Use this command for RSTP or MSTP.

This command has the same effect as the `spanning-tree portfast (STP)` command, but the configuration displays differently in the output of some show commands.

Use the **no** variant of this command to set a port to its default state (not an edge-port).

**Syntax**
```
spanning-tree edgeport
no spanning-tree edgeport
```

**Default**
Not an edge port.

**Mode**
Interface Configuration

**Usage**
Use this command on a switch port connected to a LAN that has no other bridges attached. If a BPDU is received on the port that indicates that another bridge is connected to the LAN, then the port is no longer treated as an edge port.

**Example**
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree edgeport
```

**Related Commands**
`spanning-tree autoedge (RSTP and MSTP)`
spansning-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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mstp</td>
<td>Enables or disables MSTP (Multiple Spanning Tree Protocol).</td>
</tr>
<tr>
<td>rstp</td>
<td>Enables or disables RSTP (Rapid Spanning Tree Protocol).</td>
</tr>
<tr>
<td>stp</td>
<td>Enables or disables STP (Spanning Tree Protocol).</td>
</tr>
</tbody>
</table>

**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`
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
```

**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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;10-1000000&gt;</code></td>
<td>Specify the errdisable-timeout interval in seconds.</td>
</tr>
</tbody>
</table>
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;version&gt;</td>
<td>&lt;0-3&gt; Version identifier.</td>
</tr>
<tr>
<td>0</td>
<td>Forces the port to operate in STP mode.</td>
</tr>
<tr>
<td>1</td>
<td>Not supported.</td>
</tr>
<tr>
<td>2</td>
<td>Forces the port to operate in RSTP mode. If it receives STP BPDUs, it can automatically revert to STP mode.</td>
</tr>
<tr>
<td>3</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;forward-delay&gt;</td>
<td>&lt;4-30&gt; The forwarding time delay in seconds.</td>
</tr>
</tbody>
</table>

**Default**
The default is 15 seconds.

**Mode**
Global Configuration

**Usage**
The allowable range for forward-time is 4-30 seconds.

The **forward delay**, **max-age**, and **hello time** parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

\[
2 \times (\text{forward delay} - 1.0 \text{ seconds}) \geq \text{max-age}
\]
\[
\text{max-age} \geq 2 \times (\text{hello time} + 1.0 \text{ seconds})
\]

**Example**
```
awplus# configure terminal
awplus(config)# spanning-tree forward-time 6
```

**Related Commands**
- `show spanning-tree`
- `spanning-tree forward-time`
- `spanning-tree hello-time`
- `spanning-tree mode`
**spanning-tree guard root**

**Overview**
Use this command in Interface Configuration mode for a switch port only to enable the Root Guard feature for the switch port. The root guard feature disables reception of superior BPDUs. You can use this command for RSTP, STP or MSTP. Use the **no** variant of this command to disable the root guard feature for the port.

**Syntax**
- `spanning-tree guard root`
- `no spanning-tree guard root`

**Mode**
Interface Configuration mode for a switch port interface only.

**Usage**
The Root Guard feature makes sure that the port on which it is enabled is a designated port. If the Root Guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

**Example**
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree guard root
```
spanning-tree hello-time

**Overview**

Use this command to set the hello-time. This sets the time in seconds between the transmission of device spanning tree configuration information when the device is the Root Bridge of the spanning tree or is trying to become the Root Bridge.

Use this command for RSTP, STP or MSTP.

Use the `no` variant of this command to restore the default of the hello time.

**Syntax**

```
spanning-tree hello-time <hello-time>
no spanning-tree hello-time
```

**Default**

Default is 2 seconds.

**Mode**

Global Configuration and Interface Configuration for switch ports.

**Usage**

The allowable range of values is 1-10 seconds.

The `forward delay`, `max-age`, and `hello time` parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

\[
2 \times (\text{forward delay} - 1.0 \text{ seconds}) \geq \text{max-age} \\
\text{max-age} \geq 2 \times (\text{hello time} + 1.0 \text{ seconds})
\]

**Example**

```
awplus# configure terminal
awplus(config)# spanning-tree hello-time 3
```

**Related Commands**

- `spanning-tree forward-time`
- `spanning-tree max-age`
- `show spanning-tree`
spanning-tree link-type

**Overview**  
Use this command in Interface Configuration mode for a switch port interface only to enable or disable point-to-point or shared link types on the switch port.  
Use this command for RSTP or MSTP only.  
Use the **no** variant of this command to return the port to the default link type.

**Syntax**  
```
spanning-tree link-type {point-to-point|shared}
no spanning-tree link-type
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>shared</td>
<td>Disable rapid transition.</td>
</tr>
<tr>
<td>point-to-point</td>
<td>Enable rapid transition.</td>
</tr>
</tbody>
</table>

**Default**  
The default link type is point-to-point.

**Mode**  
Interface Configuration mode for a switch port interface only.

**Usage**  
You may want to set link type to shared if the port is connected to a hub with multiple devices connected to it.

**Examples**  
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree link-type point-to-point
```
**spanning-tree max-age**

**Overview**  
Use this command to set the max-age. This sets the maximum age, in seconds, that dynamic spanning tree configuration information is stored in the device before it is discarded.

Use this command for RSTP, STP or MSTP.

Use the `no` variant of this command to restore the default of max-age.

**Syntax**

```
spanning-tree max-age <max-age>
no spanning-tree max-age
```

**Default**  
The default of spanning-tree max-age is 20 seconds.

**Mode**  
Global Configuration

**Usage**  
Max-age is the maximum time in seconds for which a message is considered valid. Configure this value sufficiently high, so that a frame generated by the root bridge can be propagated to the leaf nodes without exceeding the max-age.

The forward delay, max-age, and hello time parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

\[
2 \times (\text{forward delay} - 1.0 \text{ seconds}) \geq \text{max-age}
\]

\[
\text{max-age} \geq 2 \times (\text{hello time} + 1.0 \text{ seconds})
\]

**Example**

```
awplus# configure terminal
awplus(config)# spanning-tree max-age 12
```

**Related Commands**
- show spanning-tree
- spanning-tree forward-time
- spanning-tree hello-time
spanning-tree max-hops (MSTP)

**Overview**
Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST region. Use the no variant of this command to restore the default. Use this command for MSTP only.

**Syntax**
```
spanning-tree max-hops <hop-count>
no spanning-tree max-hops <hop-count>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;hop-count&gt;</td>
<td>Specify the maximum hops the BPDU will be valid for in the range &lt;1-40&gt;.</td>
</tr>
</tbody>
</table>

**Default**
The default max-hops in a MST region is 20.

**Mode**
Global Configuration

**Usage**
Specifying the max hops for a BPDU prevents the messages from looping indefinitely in the network. The hop count is decremented by each receiving port. When a device receives an MST BPDU that has a hop count of zero, it discards the BPDU.

**Examples**
```
awplus# configure terminal
awplus(config)# spanning-tree max-hops 25
awplus# configure terminal
awplus(config)# no spanning-tree max-hops
```
spanning-tree mode

**Overview**  Use this command to change the spanning tree protocol mode on the device. The spanning tree protocol mode on the device can be configured to either STP, RSTP or MSTP.

**Syntax**  spanning-tree mode {stp|rstp|mstp}

**Default**  The default spanning tree protocol mode on the device is RSTP.

**Mode**  Global Configuration

**Usage**  With no configuration, the device will have spanning tree enabled, and the spanning tree mode will be set to RSTP. Use this command to change the spanning tree protocol mode on the device. MSTP is VLAN aware, but RSTP and STP are not VLAN aware. To enable or disable spanning tree operation, see the spanning-tree enable command.

**Examples**  To change the spanning tree mode from the default of RSTP to MSTP, use the following commands:

awplus# configure terminal
awplus(config)# spanning-tree mode mstp

**Related Commands**  spanning-tree enable
spanning-tree mst configuration

**Overview**
Use this command to enter the MST Configuration mode to configure the Multiple Spanning-Tree Protocol.

**Syntax**
spanning-tree mst configuration

**Mode**
Global Configuration

**Examples**
The following example uses this command to enter MST Configuration mode. Note the change in the command prompt.

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)#
```
**spanning-tree mst instance**

**Overview**  Use this command in Interface Configuration mode to assign a Multiple Spanning Tree instance (MSTI) to a switch port or channel group.

Note that ports are automatically configured to send and receive spanning-tree information for the associated MSTI when VLANs are assigned to MSTIs using the `instance vlan (MSTP)` command.

Use the `no` variant of this command in Interface Configuration mode to remove the MSTI from the specified switch port or channel group.

**Syntax**  
```
spanning-tree mst instance <instance-id>
no spanning-tree mst instance <instance-id>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;instance-id&gt;</code></td>
<td><code>&lt;1-15&gt;</code> Specify the MST instance ID. The MST instance must have already been created using the <code>instance vlan (MSTP)</code> command.</td>
</tr>
</tbody>
</table>

**Default**  A port automatically becomes a member of an MSTI when it is assigned to a VLAN.

**Mode**  Interface Configuration mode for a switch port or channel group.

**Usage**  You can disable automatic configuration of member ports of a VLAN to an associated MSTI by using a `no spanning-tree mst instance` command to remove the member port from the MSTI. Use the `spanning-tree mst instance` command to add a VLAN member port back to the MSTI.

**Examples**  
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
```

**Related Commands**  
- `instance vlan (MSTP)`
- `spanning-tree mst instance path-cost`
- `spanning-tree mst instance priority`
- `spanning-tree mst instance restricted-role`
- `spanning-tree mst instance restricted-tcn`
spanning-tree mst instance path-cost

**Overview**  Use this command in Interface Configuration mode for a switch port interface only to set the cost of a path associated with a switch port, for the specified MSTI (Multiple Spanning Tree Instance) identifier.

This specifies the switch port’s contribution to the cost of a path to the MSTI regional root via that port. This applies when the port is the root port for the MSTI.

Use the `no` variant of this command to restore the default cost value of the path.

**Syntax**  
```
spanning-tree mst instance <instance-id> path-cost <path-cost>
no spanning-tree mst instance <instance-id> path-cost
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;instance-id&gt;</code></td>
<td>Specify the MSTI identifier in the range <code>&lt;1-15&gt;</code>.</td>
</tr>
<tr>
<td><code>&lt;path-cost&gt;</code></td>
<td>Specify the cost of path in the range of <code>&lt;1-200000000&gt;</code>, where a lower path-cost indicates a greater likelihood of the specific interface becoming a root.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Port speed</th>
<th>Default path cost</th>
<th>Recommended path cost range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 100 Kb/s</td>
<td>200,000,000</td>
<td>20,000,000-200,000,000</td>
</tr>
<tr>
<td>1Mbps</td>
<td>20,000,000</td>
<td>2,000,000-20,000,000</td>
</tr>
<tr>
<td>10Mbps</td>
<td>2,000,000</td>
<td>200,000-2,000,000</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>200,000</td>
<td>20,000-200,000</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>20,000</td>
<td>2-200</td>
</tr>
<tr>
<td>10 Gbps</td>
<td>2,000</td>
<td>2-200</td>
</tr>
<tr>
<td>100 Gbps</td>
<td>200</td>
<td>2-200</td>
</tr>
<tr>
<td>1Tbps</td>
<td>20</td>
<td>2-200</td>
</tr>
<tr>
<td>10 Tbps</td>
<td>2</td>
<td>2-200</td>
</tr>
</tbody>
</table>

**Mode**  Interface Configuration mode for a switch port interface only.

**Usage**  Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the spanning-tree instance command.
SPANNING TREE COMMANDS
SPANNING-TREE MST INSTANCE PATH-COST

**Examples**

```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 path-cost 1000
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3 path-cost
```

**Related Commands**

- instance vlan (MSTP)
- spanning-tree mst instance
- spanning-tree mst instance priority
- spanning-tree mst instance restricted-role
- spanning-tree mst instance restricted-tcn
spanning-tree mst instance priority

**Overview**  Use this command in Interface Configuration mode for a switch port interface only to set the port priority for an MST instance (MSTI).

Use the **no** variant of this command to restore the default priority value (128).

**Syntax**

```plaintext
spanning-tree mst instance <instance-id> priority <priority>
no spanning-tree mst instance <instance-id> [priority]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;instance-id&gt;</code></td>
<td>Specify the MSTI identifier in the range &lt;1-15&gt;.</td>
</tr>
<tr>
<td><code>&lt;priority&gt;</code></td>
<td>This must be a multiple of 16 and within the range &lt;0-240&gt;. A lower priority indicates greater likelihood of the port becoming the root port.</td>
</tr>
</tbody>
</table>

**Default**  The default is 128.

**Mode**  Interface Configuration mode for a switch port interface.

**Usage**  This command sets the value of the priority field contained in the port identifier. The MST algorithm uses the port priority when determining the root port for the switch in the MSTI. The port with the lowest value is considered to have the highest priority and will be chosen as root port over a port - equivalent in all other aspects - but with a higher priority value.

**Examples**

```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 priority 112
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3 priority
```

**Related Commands**

- instance vlan (MSTP)
- spanning-tree priority (port priority)
- spanning-tree mst instance
- spanning-tree mst instance restricted-role
- spanning-tree mst instance restricted-tcn
**spansning-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
```

### Default
The restricted role for an MSTI instance on a switch port is disabled by default.

### Mode
Interface Configuration mode for a switch port interface only.

### Usage
The root port is the port providing the best path from the bridge to the root bridge. Use this command to disable a port from becoming a root port. Use the `no` variant of this command to enable a port to become a root port. See the STP Feature Overview and Configuration Guide for root port information.

### Examples
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 restricted-role
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3 restricted-role
```

### Related Commands
- `instance vlan (MSTP)`
- `spanning-tree priority (port priority)`
- `spanning-tree mst instance`
- `spanning-tree mst instance path-cost`
- `spanning-tree mst instance restricted-tcn`
spanning-tree mst instance restricted-tcn

Overview
Use this command in Interface Configuration mode for a switch port interface only to set the restricted TCN (Topology Change Notification) value to TRUE for the specified MSTI (Multiple Spanning Tree Instance).

Use the no variant of this command in Interface Configuration mode to reset the restricted TCN for the specified MSTI to the default value of FALSE.

Syntax

```
spanning-tree mst instance <instance-id> restricted-tcn
no spanning-tree mst instance <instance-id> restricted-tcn
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;instance-id&gt;</td>
<td>&lt;1-15&gt; Specify the MST instance ID. The MST instance must have already been created using the instance vlan (MSTP) command.</td>
</tr>
</tbody>
</table>

Default
The default value for restricted TCNs is FALSE, as reset with the no variant of this command.

Mode
Interface Configuration mode for a switch port interface only.

Usage
A Topology Change Notification (TCN) is a simple Bridge Protocol Data Unit (BPDU) that a bridge sends out to its root port to signal a topology change. You can configure restricted TCN between TRUE and FALSE values with this command and the no variant of this command.

If you configure restricted TCN to TRUE with this command then this stops the switch port from propagating received topology change notifications and topology changes to other switch ports.

If you configure restricted TCN to FALSE with the no variant of this command then this enables the switch port to propagate received topology change notifications and topology changes to other switch ports.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 restricted-tcn
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3 restricted-tcn
```
SPANNING TREE COMMANDS
SPANNING-TREE MST INSTANCE 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.

<table>
<thead>
<tr>
<th>Port speed</th>
<th>Default path cost</th>
<th>Recommended path cost range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 100 Kb/s</td>
<td>200,000,000</td>
<td>20,000,000-200,000,000</td>
</tr>
<tr>
<td>1Mbps</td>
<td>20,000,000</td>
<td>2,000,000-20,000,000</td>
</tr>
<tr>
<td>10Mbps</td>
<td>2,000,000</td>
<td>200,000-2,000,000</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>200,000</td>
<td>20,000-200,000</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>20,000</td>
<td>2,000-20,000</td>
</tr>
<tr>
<td>10 Gbps</td>
<td>2,000</td>
<td>200-2,000</td>
</tr>
<tr>
<td>100 Gbps</td>
<td>200</td>
<td>20-200</td>
</tr>
<tr>
<td>1 Tbps</td>
<td>20</td>
<td>2-200</td>
</tr>
<tr>
<td>10 Tbps</td>
<td>2</td>
<td>2-20</td>
</tr>
</tbody>
</table>

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
```plaintext
spanning-tree portfast
no spanning-tree portfast
```

Default
Not an edge port.

Mode
Interface Configuration mode for a switch port interface only.

Usage
Portfast makes a port move from a blocking state to a forwarding state, bypassing both listening and learning states. The portfast feature is meant to be used for ports connected to end-user devices. Enabling portfast on ports that are connected to a workstation or server allows devices to connect to the network without waiting for spanning-tree to converge.

For example, you may need hosts to receive a DHCP address quickly and waiting for STP to converge would cause the DHCP request to time out. Ensure you do not use portfast on any ports connected to another device to avoid creating a spanning-tree loop on the network.

Use this command on a switch port that connects to a LAN with no other bridges attached. An edge port should never receive BPDUs. Therefore if an edge port receives a BPU, 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).
SPANNING TREE COMMANDS

SPANNING-TREE PORTFAST (STP)

**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
```

**Default**  
BPDU Filter is not enabled on any ports by default.

**Mode**  
Global Configuration and Interface Configuration

**Usage**  
This command filters the BPDUs and passes only data to continue to act as an edge port. Using this command in Global Configuration mode applies the portfast bpdu-filter feature to all ports on the device. Using it in Interface mode applies the feature to a specific port, or range of ports. The command will operate in both RSTP and MSTP networks.

Use the `show spanning-tree` command to display status of the bpdu-filter parameter for the switch ports.

**Example**  
To enable STP BPDU filtering in Global Configuration mode, enter the commands:
```
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-filter
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bpdu-filter</td>
<td>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):</td>
</tr>
<tr>
<td>default</td>
<td>Takes the setting that has been configured for the whole device, i.e. the setting made from the Global configuration mode.</td>
</tr>
<tr>
<td>disable</td>
<td>Turns off BPDU filter.</td>
</tr>
<tr>
<td>enable</td>
<td>Turns on BPDU filter.</td>
</tr>
</tbody>
</table>
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
```

Default
BPDU Guard is not enabled on any ports by default.

Mode
Global Configuration or Interface Configuration

Usage
This command blocks the port(s) to all devices and data when enabled. BPDU Guard is a port-security feature that changes how a portfast-enabled port behaves if it receives a BPDU. When bpdu-guard is set, then the port shuts down if it receives a BPDU. It does not process the BPDU as it is considered suspicious. When bpdu-guard is not set, then the port will negotiate spanning-tree with the device sending the BPDUs. By default, bpdu-guard is not enabled on a port.

You can configure a port disabled by the bpdu-guard to re-enable itself after a specific time interval. This interval is set with the spanning-tree errdisable-timeout interval command. If you do not use the errdisable-timeout feature, then you will need to manually re-enable the port by using the no shutdown command.
Use the `show spanning-tree` command to display the device and port configurations for the BPDU Guard feature. It shows both the administratively configured and currently running values of bpdu-guard.

**Example**

To enable STP BPDU guard in Global Configuration mode, enter the below commands:
```
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-guard
```

To enable STP BPDU guard in Interface Configuration mode, enter the below commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree portfast bpdu-guard enable
```

**Related Commands**

- `spanning-tree edgeport` (RSTP and MSTP)
- `show spanning-tree`
- `spanning-tree portfast` (STP)
- `spanning-tree portfast bpdu-filter`
**spanning-tree priority (bridge priority)**

**Overview**  Use this command to set the bridge priority for the device. A lower priority value indicates a greater likelihood of the device becoming the root bridge.

Use this command for RSTP, STP or MSTP. When MSTP mode is configured, this will apply to the CIST.

Use the `no` variant of this command to reset it to the default.

**Syntax**

```
spanning-tree priority <priority>
no spanning-tree priority
```

**Default**  The default priority is 32768.

**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
```

**Default**
The default priority is 128.

**Mode**
Interface Configuration mode for a switch port interface only.

**Usage**
To force a port to be part of the active topology (for instance, become the root port or a designated port) use a lower value than other ports on the device. (This behavior is subject to network topology, and more significant factors, such as bridge ID.)

**Example**
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree priority 16
```

**Related Commands**
- `spanning-tree mst instance priority`
- `spanning-tree priority (bridge priority)`
- `show spanning-tree`
spanning-tree restricted-role

**Overview**  
Use this command in Interface Configuration mode for a switch port interface only to restrict the port from becoming a root port.  

Use the `no` variant of this command to disable the restricted role functionality.

**Syntax**  
- spanning-tree restricted-role  
- no spanning-tree restricted-role

**Default**  
The restricted role is disabled.

**Mode**  
Interface Configuration mode for a switch port interface only.

**Example**  
```bash  
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.
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.

Link aggregation hashes one or more of the source and destination MAC address, IP address and UDP/TCP ports to select a link on which to send a packet. So packet flow between a pair of hosts always takes the same link inside the Link Aggregation Group (LAG). The net effect is that the bandwidth for a given packet stream is restricted to the speed of one link in the LAG.

For example, for a 2 Gbps LAG that is a combination of two 1 Gbps ports, any one flow of traffic can only ever reach a maximum throughput of 1 Gbps. However, the hashing algorithm should spread the flows across the links so that when many flows are operating, the full 2 Gbps can be utilized.

For a description of static and dynamic link aggregation (LACP), and configuration examples, see the Link Aggregation Feature Overview and Configuration Guide.
LINK AGGREGATION COMMANDS

Command List

- “channel-group” on page 573
- “clear lacp counters” on page 575
- “debug lacp” on page 576
- “lacp port-priority” on page 577
- “lacp system-priority” on page 578
- “lacp timeout” on page 579
- “show debugging lacp” on page 581
- “show diagnostic channel-group” on page 582
- “show etherchannel” on page 584
- “show etherchannel detail” on page 585
- “show etherchannel summary” on page 586
- “show lacp sys-id” on page 587
- “show lacp-counter” on page 588
- “show port etherchannel” on page 589
- “show static-channel-group” on page 591
- “static-channel-group” on page 592
- “undebug lacp” on page 594
channel-group

**Overview**
Use this command to add the device port to a dynamic channel group specified by the dynamic channel group number, and set its mode. This command enables LACP link aggregation on the device port, so that it may be selected for aggregation by the local system. Dynamic channel groups are also known as LACP channel groups, LACP aggregators or etherchannels.

You can create up to 32 dynamic (LACP) channel groups (and up to 96 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;dynamic-channel-group-number&gt;</code></td>
<td>&lt;1-32&gt; Specify a dynamic channel group number for an LACP link. You can create up to 32 dynamic (LACP) channel groups (as well as up to 96 static channel groups).</td>
</tr>
<tr>
<td><code>active</code></td>
<td>Enables initiation of LACP negotiation on a port. The port will transmit LACP dialogue messages whether or not it receives them from the partner system.</td>
</tr>
<tr>
<td><code>passive</code></td>
<td>Disables initiation of LACP negotiation on a port. The port will only transmit LACP dialogue messages if the partner systems is transmitting them, i.e., the partner is in the active mode.</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration

**Usage**
All the device ports in a channel-group must belong to the same VLANs, have the same tagging status, and can only be operated on as a group. All device ports within a channel group must have the same port speed and be in full duplex mode.

Once the LACP channel group has been created, it is treated as a device port, and can be referred to in most other commands that apply to device ports.

To refer to an LACP channel group in other LACP commands, use the channel group number. To specify an LACP channel group (LACP aggregator) in other commands, prefix the channel group number with `po`. For example, `po2` refers to the LACP channel group with channel group number 2.

For more information about LACP, see the Link Aggregation Feature Overview and Configuration Guide.
**Examples**

To add device `port1.0.6` to a newly created LACP channel group 2 use the commands below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# channel-group 2 mode active
```

To remove device `port1.0.6` from any created LACP channel groups use the command below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no channel-group
awplus(config)#
```

To reference the pre-defined LACP channel group 2 as an interface, apply commands as below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# channel-group 2 mode active
awplus(config-if)# exit
awplus(config)# interface port1.0.6
awplus(config-if)# channel-group 2 mode active
awplus(config-if)# exit
awplus(config)# interface po2
awplus(config-if)#
```

**Related Commands**

- `show etherchannel`
- `show etherchannel detail`
- `show etherchannel summary`
- `show port etherchannel`
clear lACP counters

**Overview**  Use this command to clear all counters of all present LACP aggregators (channel groups) or a given LACP aggregator.

**Syntax**
```
clear lacp [<1-32>] counters
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-32&gt;</td>
<td>Channel-group number.</td>
</tr>
</tbody>
</table>

**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]}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Turn on all debugging for LACP.</td>
</tr>
<tr>
<td>cli</td>
<td>Specifies debugging for CLI messages. Echoes commands to the console.</td>
</tr>
<tr>
<td>event</td>
<td>Specifies debugging for LACP events. Echoes events to the console.</td>
</tr>
<tr>
<td>ha</td>
<td>Specifies debugging for HA (High Availability) events. Echoes High Availability events to the console.</td>
</tr>
<tr>
<td>packet</td>
<td>Specifies debugging for LACP packets. Echoes packet contents to the console.</td>
</tr>
<tr>
<td>sync</td>
<td>Specified debugging for LACP synchronization. Echoes synchronization to the console.</td>
</tr>
<tr>
<td>timer</td>
<td>Specifies debugging for LACP timer. Echoes timer expiry to the console.</td>
</tr>
<tr>
<td>detail</td>
<td>Optional parameter for LACP timer-detail. Echoes timer start/stop details to the console.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec and Global Configuration

**Examples**
```
awplus# debug lacp timer detail
awplus# debug lacp all
```

**Related Commands**
- `show debugging lacp`
- `undebug lacp`
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Specify the LACP port priority.</td>
</tr>
</tbody>
</table>

**Default**
The default is 32768.

**Mode**
Interface Configuration

**Example**

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# lacp port-priority 34
```
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>LACP system priority. Lower numerical values have higher priorities.</td>
</tr>
</tbody>
</table>

**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
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.

```bash
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lACP timeout short
```
**show debugging lacp**

**Overview**  
Use this command to display the LACP debugging option set.  
For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
`show debugging lacp`

**Mode**  
User Exec and Privileged Exec

**Example**  
`awplus# show debugging lacp`

**Output**  
Figure 13-1: Example output from the `show debugging lacp` command

```
LACP debugging status:
LACP timer debugging is on
LACP timer-detail debugging is on
LACP cli debugging is on
LACP packet debugging is on
LACP event debugging is on
LACP sync debugging is on
```

**Related Commands**  
`debug lacp`
show diagnostic channel-group

**Overview**
This command displays dynamic and static channel group interface status information. The output of this command is useful for Allied Telesis authorized service personnel for diagnostic purposes.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show diagnostic channel-group
```

**Mode**
User Exec and Privileged Exec

**Example**
```
awplus# show diagnostic channel-group
```
Output

Figure 13-2: Example output from the `show diagnostic channel-group` command

```bash
awplus#show diagnostic channel-group

Channel Group Info based on NSM:
Note: Pos - position in hardware table

+-----------------+----------+----------+-----------+----------+----------+------+
| Dev         | Interface| IfIndex  | Member    | 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    | 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    | 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    | 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 a LACP channel specified by the channel group number.

The command output also shows the thrash limiting status. If thrash limiting is detected and the `thresh limiting` parameter of the `thresh-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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**

```
show etherchannel [<1-32>]
```

**Mode**

User Exec and Privileged Exec

**Example**

```
awplus# show etherchannel 2
```

**Output**

Figure 13-3: Example output from the `show etherchannel` command for a particular channel

```<LC>
% LACP Aggregator: po1

Thrash-limiting

Status Vlan Thrashing Detected, Action vlan-disable 60(s)

Thrashing Vlans 1 2 3 4 5
% Member:
  port1.0.4
  port1.0.6
```
**show etherchannel detail**

**Overview**  Use this command to display detailed information about all LACP channels. For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show etherchannel detail

**Mode**  User Exec and Privileged Exec

**Example**  awplus# show etherchannel detail

**Output**  Figure 13-4: Example output from the show etherchannel detail command

```plaintext
Aggregator po1 (IfIndex: 4501)
  Mac address: 00:00:cd:24:fd:29
  Admin Key: 0001 - Oper Key 0001
  Receive link count: 1 - Transmit link count: 0
  Individual: 0 - Ready: 1
  Partner LAG: 0x8000,00-00-cd-24-da-a7
    Link: port1.0.1 (IfIndex: 5001) disabled
    Link: port1.0.2 (IfIndex: 5002) sync: 1
Aggregator po2 (IfIndex: 4502)
  Mac address: 00:00:cd:24:fd:29
  Admin Key: 0002 - Oper Key 0002
  Receive link count: 1 - Transmit link count: 0
  Individual: 0 - Ready: 1
  Partner LAG: 0x8000,00-00-cd-24-da-a7
    Link: port1.0.6 (IfIndex: 5007) disabled
```
**show etherchannel summary**

**Overview**  Use this command to display a summary of all LACP channels.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show etherchannel summary

**Mode**  User Exec and Privileged Exec

**Example**  awplus# show etherchannel summary

**Output**  Figure 13-5: Example output from the show etherchannel summary command

```plaintext
% Aggregator po1
%  Admin Key: 0001 - Oper Key 0001
%  Link: port1.0.1 (5001) disabled
%  Link: port1.0.2 (5002) sync: 1
% Aggregator po2
%  Admin Key: 0002 - Oper Key 0002
%  Link: port1.0.6 (5007) disabled
```
show lacp sys-id

**Overview**  Use this command to display the LACP system ID and priority.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  

show lacp sys-id

**Mode**  

User Exec and Privileged Exec

**Example**  

awplus# show lacp sys-id

**Output**  

Figure 13-6: Example output from the `show lacp sys-id` command

```
System Priority: 0x8000 (32768)
MAC Address: 0200.0034.5684
```
show lacp-counter

**Overview** Use this command to display the packet traffic on all ports of all present LACP aggregators, or a given LACP aggregator.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**

```
show lacp-counter [<1-32>]
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-32&gt;</td>
<td>Channel-group number.</td>
</tr>
</tbody>
</table>

**Mode** User Exec and Privileged Exec

**Example**

```
awplus# show lacp-counter 2
```

**Output** Figure 13-7: Example output from the `show lacp-counter` command

```
% Traffic statistics
Port          LACPDUs         Marker         Pckt err
Sent    Recv    Sent    Recv    Sent    Recv
% Aggregator po2 (IfIndex: 4604)
port1.0.2   0       0       0       0       0       0
```
show port etherchannel

**Overview**  Use this command to show LACP details of the device port specified.
For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show port etherchannel <port>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>Name of the device port to display LACP information about.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**  awplus# show port etherchannel port1.0.1

**Output**  Figure 13-8:  Example output from the `show port etherchannel` command
**Link Aggregation Commands**

**SHOW PORT ETHERCHANNEL**

<table>
<thead>
<tr>
<th>Link:</th>
<th>port1.0.1 (5001)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregator:</td>
<td>po1 (4501)</td>
</tr>
<tr>
<td>Receive machine state:</td>
<td>Current</td>
</tr>
<tr>
<td>Periodic Transmission machine state:</td>
<td>Fast periodic</td>
</tr>
<tr>
<td>Mux machine state:</td>
<td>Collecting/Distributing</td>
</tr>
</tbody>
</table>

**Actor Information:**

<table>
<thead>
<tr>
<th>Actor Information:</th>
<th>Partner Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected ..........</td>
<td>Selected .............</td>
</tr>
<tr>
<td>Physical Admin Key</td>
<td>1</td>
</tr>
<tr>
<td>Port Key ...........</td>
<td>5</td>
</tr>
<tr>
<td>Port Priority ......</td>
<td>32768</td>
</tr>
<tr>
<td>Port Number ..,...,</td>
<td>5001</td>
</tr>
<tr>
<td>Mode ...............</td>
<td>Active ................</td>
</tr>
<tr>
<td>Timeout ............</td>
<td>Long ..................</td>
</tr>
<tr>
<td>Individual ..........</td>
<td>Yes</td>
</tr>
<tr>
<td>Synchronised .......</td>
<td>Yes</td>
</tr>
<tr>
<td>Collecting ..........</td>
<td>Yes</td>
</tr>
<tr>
<td>Distributing .......</td>
<td>Yes</td>
</tr>
<tr>
<td>defaulted ..........</td>
<td>Yes</td>
</tr>
<tr>
<td>Expired ................</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Partner Information:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner Sys Priority</td>
<td>0</td>
</tr>
<tr>
<td>Partner System ..</td>
<td>00-00-00-00-00-00</td>
</tr>
<tr>
<td>Port Key ...........</td>
<td>0</td>
</tr>
<tr>
<td>Port Priority ......</td>
<td>0</td>
</tr>
<tr>
<td>Port Number ..,...,</td>
<td>0</td>
</tr>
<tr>
<td>Mode ...............</td>
<td>Passive ............</td>
</tr>
<tr>
<td>Timeout ............</td>
<td>Short ..............</td>
</tr>
<tr>
<td>Individual ..........</td>
<td>No</td>
</tr>
<tr>
<td>Synchronised .......</td>
<td>No</td>
</tr>
<tr>
<td>Collecting ..........</td>
<td>No</td>
</tr>
<tr>
<td>Distributing .......</td>
<td>No</td>
</tr>
<tr>
<td>Defaulted ..........</td>
<td>No</td>
</tr>
<tr>
<td>Expired ................</td>
<td>No</td>
</tr>
</tbody>
</table>
**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 `thrash limiting` 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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
`show static-channel-group`

**Mode**  
User Exec and Privileged Exec

**Example**  
```
awplus# show static-channel-group
```

**Output**  
Figure 13-9: Example output from the `show static-channel-group` command

```
% LAG Maximum : 128
% LAG Static Maximum: 96
% LAG Dynamic Maximum: 32
% LAG Static Count : 2
% LAG Dynamic Count : 2
% LAG Total Count : 4
% Static Aggregator: sa2
% Member:
  port1.0.1
% Static Aggregator: sa3
% Member:
  port1.0.2
```

**Related Commands**  
`static-channel-group`
static-channel-group

**Overview**
Use this command to create a static channel group, also known as a static aggregator, or add a member port to an existing static channel group.

You can create up to 96 static channel groups (and up to 32 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;static-channel-group-number&gt;</code></td>
<td><code>&lt;1-96&gt;</code> Static channel group number.</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration

**Usage**
This command adds the device port to the static channel group with the specified channel group number. If the channel group does not exist, it is created, and the port is added to it. The **no** prefix detaches the port from the static channel group. If the port is the last member to be removed, the static channel group is deleted.

All the ports in a channel group must have the same VLAN configuration: they must belong to the same VLANs and have the same tagging status, and can only be operated on as a group.

Once the static channel group has been created, it is treated as a device port, and can be referred to in other commands that apply to device ports.

To refer to a static channel group in other static channel group commands, use the channel group number. To specify a static channel group in other commands, prefix the channel group number with **sa**. For example, 'sa2' refers to the static channel group with channel group number 2.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Examples**
To define a static channel group on a device port, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# static-channel-group 2
```
To reference the pre-defined static channel group 2 as an interface apply the example commands as below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface port1.0.8
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface sa2
awplus(config-if)#
```

Related Commands

- `show static-channel-group`
**Overview**  This command applies the functionality of the `no debug lACP` command.
Introduction

Overview

This chapter contains an alphabetical list of commands used to configure Power over Ethernet (PoE). Each command contains a functional description and shows examples of configuration and output screens for show commands. These commands are only supported on PoE capable ports. An error message will display on the console if you enter a PoE command on a port that does not support PoE. The following documents offer further information for configuring PoE on AlliedWare Plus switches:

- the PoE Feature Overview and Configuration Guide.
- the SNMP MIBs Overview, for information about which PoE MIB objects are supported.
- the SNMP Feature Overview and Configuration Guide, for information about SNMP traps.

Power over Ethernet (PoE) is a technology allowing devices such as IP phones to receive power over existing LAN cabling.

PoE is configured using the commands in this chapter. Note the Power Sourcing Equipment (PSE) referred to throughout this chapter is an Allied Telesis PoE switch running the AlliedWare Plus™ Operating System, supporting the IEEE 802.3af and IEEE 802.3at Power Ethernet standards. The Powered Device (PD) referred to throughout this chapter is a PoE or PoE+ powered device, such as an IP phone or a Wireless Access Point (WAP).

The commands in this chapter are available on the Allied Telesis x510-52GPX and x510-28GPX switches:

**NOTE:**

**NOTE:**
Command List

- “clear power-inline counters interface” on page 596
- “debug power-inline” on page 597
- “power-inline allow-legacy” on page 599
- “power-inline description” on page 600
- “power-inline enable” on page 601
- “power-inline max” on page 602
- “power-inline priority” on page 604
- “power-inline usage-threshold” on page 606
- “service power-inline” on page 607
- “show debugging power-inline” on page 608
- “show power-inline” on page 609
- “show power-inline counters” on page 612
- “show power-inline interface” on page 614
- “show power-inline interface detail” on page 616
clear power-inline counters interface

**Overview**
This command will clear the counters from a specified port, a range of ports, or all ports on the Power Sourcing Equipment (PSE). If no ports are entered then PoE counters for all ports are cleared. It will also clear all Power over Ethernet (PoE) counters supported by the Power Ethernet MIB (RFC 3621).

**Syntax**
clear power-inline counters interface [port-list]

**Mode**
Privileged Exec

**Usage**
The PoE counters are displayed with the show power-inline counters command.

**Examples**
To clear the PoE counters for port1.0.2 only, use the following command:
awplus# clear power-inline counters interface port1.0.2

To clear the PoE counters for port1.0.1 through port1.0.10, use the following command:
awplus# clear power-inline counters interface port1.0.1-port1.0.10

To clear the PoE counters for all ports, use the following command:
awplus# clear power-inline counters interface

**Validation Commands**
show power-inline counters
**debug power-inline**

**Overview**  This command enables debugging display for messages that are specific to Power over Ethernet (PoE).

Use the `no` variant of this command to disable the specified PoE debugging messages.

**Syntax**  
```
debug power-inline [all|event|info|power]
noc debug power-inline [all|event|info|power]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all (event, info, nsm, power) debug messages.</td>
</tr>
<tr>
<td>event</td>
<td>Displays event debug information, showing any error conditions that may occur during PoE operation.</td>
</tr>
<tr>
<td>info</td>
<td>Displays informational level debug information, showing high-level essential debugging, such as information about message types.</td>
</tr>
<tr>
<td>power</td>
<td>Displays power management debug information.</td>
</tr>
</tbody>
</table>

**Default**  No debug messages are enabled by default.

**Mode**  Privileged Exec

**Usage**  Use the `terminal monitor` command to display PoE debug messages on the console.

Use the `show debugging power-inline` command to show the PoE debug configuration.

**Examples**  To enable PoE debugging and start the display of PoE event and info debug messages on the console, use the following commands:
```
awplus# terminal monitor
awplus# debug power-inline event info
```

To enable PoE debugging and start the display of all PoE debugging messages on the console, use the following commands:
```
adplus# terminal monitor
adplus# debug power-inline all
```

To disable PoE debugging and stop the display of PoE event and info debug messages on the console, use the following command:
```
awplus# no debug power-inline event info
```

To disable all PoE debugging and stop the display of any PoE debugging messages on the console, use the following command:
```
awplus# no debug power-inline all
```
POWER OVER ETHERNET COMMANDS
DEBUG POWER-INLINE

Validation Commands
show debugging power-inline

Related Commands
terminal monitor
**power-inline allow-legacy**

**Overview**
This command enables detection of pre-IEEE 802.3af Power Ethernet standard legacy Powered Devices (PDs).

The no variant of this command disables detection of pre-IEEE 802.3af Power Ethernet standard legacy Powered Devices (PDs).

**Syntax**
```
power-inline allow-legacy
no power-inline allow-legacy
```

**Default**
Detection of legacy PDs is enabled on all ports on the Power Sourcing Equipment (PSE).

**Mode**
Global Configuration

**Examples**
To disable detection of legacy PDs, use the following commands:
```
awplus# configure terminal
awplus(config)# no power-inline allow-legacy
```

To enable detection of legacy PDs, use the following commands:
```
awplus# configure terminal
awplus(config)# power-inline allow-legacy
```

**Validation Commands**
```
show power-inline
show running-config power-inline
```
**power-inline description**

**Overview**  
This command adds a description for a Powered Device (PD) connected to a PoE port.

The **no** variant of this command clears a previously entered description for a connected PD, resetting the PD description to the default (null).

**Syntax**  
```
power-inline description <pd-description>
no power-inline description
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;pd-description&gt;</code></td>
<td>Description of the PD connected to the PoE capable port (with a maximum 256 character string limit per PD description).</td>
</tr>
</tbody>
</table>

**Default**  
No description for a connected PD is set by default.

**Mode**  
Interface Configuration

**Usage**  
Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding `interface (to configure)` command. If you specify a range or list of ports they must all be PoE capable ports.

**Examples**  
To add the description Desk Phone for a connected PD on port1.0.2, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline description Desk Phone
```

To clear the description as added above for the connected PD on port1.0.2, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no power-inline description
```

**Validation Commands**  
- `show power-inline interface`
- `show running-config power-inline`
power-inline enable

**Overview**
This command enables Power over Ethernet (PoE) to detect a connected Powered Device (PD) and supply power from the Power Sourcing Equipment (PSE).

The **no** variant of this command disables PoE functionality on the selected PoE port(s). No power is supplied to a connected PD after PoE is disabled on the selected PoE port(s).

**Syntax**
```
power-inline enable
no power-inline enable
```

**Default**
PoE is enabled by default on all ports on the PSE.

**Mode**
Interface Configuration

**Usage**
In a stack of x510 Series switches this command is supported on all PoE capable ports.

Select a PoE port, a list of PoE ports, or a range of PoE ports from the preceding `interface (to configure)` command. If you specify a range or list of ports they must all be PoE capable ports.

No PoE log messages are generated for specified PoE port(s) after PoE is disabled. The disabled PoE port(s) still provide Ethernet connectivity after PoE is disabled.

**Examples**
To disable PoE on ports `port1.0.1` to `port1.0.4`, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# no power-inline enable
```

To enable PoE on ports `port1.0.1` to `port1.0.4`, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# power-inline enable
```

**Validation Commands**
- `show power-inline`
- `show power-inline interface`
- `show power-inline interface detail`
- `show running-config power-inline`
POWER OVER ETHERNET COMMANDS
POWER INLINE MAX

**power-inline max**

**Overview**  
NOTE:

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.

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
```

**Default**
The Power Sourcing Equipment (PSE) supplies the maximum power limit for the class of the PD connected to the port by default.

NOTE: See the PoE Feature Overview and Configuration Guide for further information about power classes.

**Mode**
Interface Configuration

**Usage**
In a stack of x510 Series switches this command is supported on all PoE capable ports.

Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding interface (to configure) command. If you specify a range or list of ports they must all be PoE capable ports.

If you select a range of PoE ports in Interface Configuration mode before issuing this command, then each port in the range selected will have the same maximum power value configured. If the PoE port attempts to draw more than the maximum power, this is logged and all power is removed. Note that the value entered is rounded up to the next value supported by the hardware.

See the actual value used, as shown after command entry, in the sample console output below:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;4000-30000 &gt;</td>
<td>The maximum power allocated to a PoE port in milliwatts (mW).</td>
</tr>
</tbody>
</table>
POWER OVER ETHERNET COMMANDS
POWER-INLINE MAX

See the LLDP Feature Overview and Configuration Guide for information about power monitoring at the PD.

Note the difference in power supplied from the PSE to the power available at the PD due to line loss.

See the PoE Feature Overview and Configuration Guide for further information about the difference between the power supplied from the PSE and the power available at the PD.

Examples

To set the maximum power supplied to ports in the range 1.0.2 to 1.0.4 to 6450mW per port, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# power-inline max 6450
```

To set the maximum power supplied to port 1.0.2, to 6450 mW, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline max 6450
```

To clear the user-configured maximum power supplied to port 1.0.2, and revert to using the default maximum power of 30000 mW, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no power-inline max
```

Validation Commands

```
show power-inline interface
show running-config power-inline
```
**power-inline priority**

**Overview**  
This command sets the Power over Ethernet (PoE) priority level of a PoE port to one of three available priority levels:

- **low**
- **high**
- **critical**

The **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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>low</td>
<td>The lowest priority for a PoE enabled port (default). PoE ports set to <em>low</em> only receive power if all the PoE ports assigned to the other two levels are already receiving power.</td>
</tr>
<tr>
<td>high</td>
<td>The second highest priority for a PoE enabled port. PoE ports set to <em>high</em> receive power only if all the ports set to <em>critical</em> are already receiving power.</td>
</tr>
<tr>
<td>critical</td>
<td>The highest priority for a PoE enabled port. PoE ports set to <em>critical</em> 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.</td>
</tr>
</tbody>
</table>

**Default**  
The default priority is **low** for all PoE ports on the Power Sourcing Equipment (PSE).

**Mode**  
**Interface Configuration**

**Usage**  
This command is supported on all PoE capable ports, whether operating as a stand-alone switch, or within a VCStack.

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.
**POWER OVER ETHERNET COMMANDS**

**POWER-INLINE PRIORITY**

**Examples**

To set the priority level to **high** for port1.0.2, use the following commands:

```bash
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline priority high
```

To reset the priority level to the default for port1.0.2, use the following commands:

```bash
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no power-inline priority
```

**Validation Commands**

- `show power-inline`
- `show power-inline interface`
- `show running-config power-inline`

**Related Commands**

- `power-inline usage-threshold`
power-inline usage-threshold

**Overview**  This command sets the level at which the Power Sourcing Equipment (PSE) will issue a message that the power supplied to all Powered Devices (PDs) has reached a critical level of the nominal power rating for the PSE. The level is set as a percentage of total available power.

The **no** variant of this command resets the notification usage-threshold to the default (80% of the nominal power rating of the PSE).

**Syntax**  
```
power-inline usage-threshold <1-99>
no power-inline usage-threshold
```

**Default**  The default power usage threshold is 80% of the nominal power rating of the PSE.

**Mode**  Global Configuration

**Usage**  Use the `snmp-server enable trap` command to configure SNMP notification. An SNMP notification is sent when the usage-threshold, as configured in the example, is exceeded.

**Examples**  To generate SNMP notifications when power supplied exceeds 70% of the nominal PSE power, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap power-inline
awplus(config)# power-inline usage-threshold 70
```

To reset the notification threshold to the default (80% of the nominal PSE power rating), use the following commands:

```
awplus# configure terminal
awplus(config)# no power-inline usage-threshold
```

**Validation Commands**  
- `show power-inline interface`
- `show running-config power-inline`

**Related Commands**  
- `snmp-server enable trap`
service power-inline

**Overview**  This command enables Power over Ethernet (PoE) globally on the Power Sourcing Equipment (PSE) for all PoE ports.

**Syntax**  
```
  service power-inline

  no service power-inline
```

**Default**  PoE functionality is enabled by default on the PSE.

**Mode**  Global Configuration

**Usage**  In a stack, issuing this command enables PoE globally for all PoE ports. In a stack configuration, only stack members containing PoE hardware will have PoE enabled by default in software.

**Examples**  To disable PoE on the PSE, use the following commands:

```
awplus# configure terminal
awplus(config)# no service power-inline
```

To re-enable PoE on the PSE, if PoE has been disabled, use the following commands:

```
awplus# configure terminal
awplus(config)# service power-inline
```

**Validation Commands**  
- `show power-inline`
- `show running-config power-inline`
**show debugging power-inline**

**Overview**  
This command displays Power over Ethernet (PoE) debug settings.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
`show debugging power-inline`

**Mode**  
User Exec and Privileged Exec

**Example**  
To display PoE debug settings, use the following command:

```
awplus# show debugging power-inline
```

**Output**  
Figure 14-1: Example output from the `show debugging power-inline` command

```
awplus#show debugging power-inline
PoE Debugging status:
Poe Informational debugging is disabled
Poe Event debugging is disabled
Poe Power Management debugging is disabled
Poe NSM debugging is enabled
```

**Related Commands**  
debug power-inline
terminal monitor
show power-inline

**Overview**  This command displays the Power over Ethernet (PoE) status for all ports on the Power Sourcing Equipment (PSE).

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show power-inline

**Mode**  User Exec and Privileged Exec

**Example**  To display the PoE status for all ports on the PSE, use the following command:

```
awplus# show power-inline
```

**Output**  Figure 14-2:  Example output from the `show power-inline` command

```
awplus#show power-inline
PoE Status:
  Stack Member 2
  Nominal Power: 370W
  Power Allocated: 246W

  Actual Power Consumption: 151W
  Operational Status: On
  Power Usage Threshold: 80% (296W)

PoE Interface:
  Interface  Admin   Pri  Oper    Power   Device    Class  Max(mW)
  port2.0.1  Enabled Low  Powered 3840   n/a          1    4000 [C]
  port2.0.2  Enabled High Powered 6720   n/a          2    7000 [C]
  port2.0.3  Enabled Low Powered 14784   n/a          3   15400 [C]
  port2.0.4  Enabled Crit Powered 14784   n/a          3   15400 [C]
  port2.0.5  Enabled Crit Powered 3840   n/a          1    4000 [C]
  port2.0.6  Enabled High Powered 6720   n/a          2    7000 [C]
  port2.0.7  Enabled Low Powered 14784   n/a          3   15400 [C]
```

Table 14-1:  Parameters in the `show power-inline` command output

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nominal Power</td>
<td>The nominal power available on the switch in watts (W).</td>
</tr>
<tr>
<td>Power Allocated</td>
<td>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.</td>
</tr>
<tr>
<td>Actual Power Consumption</td>
<td>The current power consumption in watts (W) drawn by all connected Powered Devices (PDs). This is updated every 5 seconds.</td>
</tr>
</tbody>
</table>
Table 14-1: Parameters in the **show power-inline** command output (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Status</td>
<td>The operational status of the PSU hardware on the PSE when this command was issued:</td>
</tr>
<tr>
<td></td>
<td>• <strong>On</strong> if the PSU as installed inside the PSE is switched on.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong> when the PSU in the PSE is switched off (an RPS may be connected to the PSE to power PoE instead of the PSU).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fault</strong> when there is an issue with the PSE PSU hardware.</td>
</tr>
<tr>
<td>Power Usage Threshold (%)</td>
<td>The configured SNMP trap / log threshold for the PSE, as configured from a <strong>power-inline usage-threshold</strong> command.</td>
</tr>
<tr>
<td>Interface</td>
<td>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.</td>
</tr>
<tr>
<td>Admin</td>
<td>The administrative state of PoE on a PoE port, either <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Pri</td>
<td>The current PoE priorities for PoE ports on the PSE, as configured from a <strong>power-inline priority</strong> command:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low</strong> displays when the low parameter is issued. The lowest priority for a PoE enabled port (default).</td>
</tr>
<tr>
<td></td>
<td>• <strong>High</strong> displays when the high parameter is issued. The second highest priority for a PoE enabled port.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Crit</strong> displays when the critical parameter is issued. The highest priority for a PoE enabled port.</td>
</tr>
<tr>
<td>Oper</td>
<td>The current PSE PoE port state when this command was issued:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Powered</strong> displays when there is a PD connected and power is being supplied from the PSE.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> displays when supplying power would make the PSE go over the power budget.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong> displays when PoE has been disabled for the PoE port.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fault</strong> displays when a PSE goes over its power allocation.</td>
</tr>
<tr>
<td>Power</td>
<td>The power consumption in milliwatts (mW) for the PoE port when this command was entered.</td>
</tr>
<tr>
<td>Device</td>
<td>The description of the connected PD device if a description has been added with the <strong>power-inline description</strong> command. No description is shown for PDs not configured with the <strong>power-inline description</strong> command.</td>
</tr>
</tbody>
</table>
Table 14-1: Parameters in the **show power-inline** command output (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>The class of the connected PD, if power is being supplied to the PD from the PSE. See the <em>Power over Ethernet Introduction</em> chapter for further information about PD classes and the power levels assigned per class.</td>
</tr>
</tbody>
</table>
| 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. |

**Related Commands**
- `show power-inline counters`
- `show power-inline interface`
show power-inline counters

**Overview**
This command displays Power over Ethernet (PoE) event counters for ports on the Power Sourcing Equipment (PSE). The PoE event counters displayed can also be accessed by objects in the PoE MIB (RFC 3621). See the MIB Objects Feature Overview and Configuration Guide for information about which PoE MIB objects are supported.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show power-inline counters [<port-list>]
```

**Mode**
User Exec and Privileged Exec

**Usage**
To display all PoE event counters for all PoE ports on the PSE, do not enter the optional interface parameter.

**Examples**
To display all PoE event counters for all PoE ports on the PSE, use the command:
```
awplus# show power-inline counters
```

To display the PoE event counters for the port range 1.0.1 to 1.0.3, use the command:
```
awplus# show power-inline counters interface port1.0.1-1.0.3
```

**Output**
Figure 14-3: Example output from the **show power-inline counters** command

```
awplus#show power-inline counters interface port1.0.4-port1.0.12
PoE Counters:
  Interface   MPSAbsent Overload Short Invalid Denied
  port1.0.4   0         0        0     0       0
  port1.0.5   0         0        0     0       0
  port1.0.6   0         0        0     0       0
  port1.0.7   0         0        0     0       0
  port1.0.8   0         0        0     0       0
  port1.0.9   0         0        0     0       0
  port1.0.10  0         0        0     0       0
  port1.0.11  0         0        0     0       0
  port1.0.12  0         0        0     0       0
```
Table 14-2: Parameters in the `show power-inline counters` command output

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The PoE port(s) in the format <code>portx.y.z</code>, where <code>x</code> is the device number, <code>y</code> is the module number within the device, and <code>z</code> is the PoE port number within the module.</td>
</tr>
<tr>
<td>MPSAbsent</td>
<td>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 <code>pethPsePortMPSAbsentCounter</code> in the PoE MIB.</td>
</tr>
<tr>
<td>Overload</td>
<td>The number of instances when a PD exceeds its configured power limit (as configured by the <code>power-inline max</code> command). Also increments <code>pethPsePortOverLoadCounter</code> in the PoE MIB.</td>
</tr>
<tr>
<td>Short</td>
<td>The number of short circuits that have happened with a PD. Also increments <code>pethPsePortShortCounter</code> in the PoE MIB.</td>
</tr>
<tr>
<td>Invalid</td>
<td>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 <code>pethPseInvalidSignatureCounter</code> in the PoE MIB.</td>
</tr>
<tr>
<td>Denied</td>
<td>The number of times a PD has been refused power due to power budget limitations for the PSE. Also increments <code>pethPsePortPowerDeniedCounter</code> in the PoE MIB.</td>
</tr>
</tbody>
</table>

Related Commands

- `clear power-inline counters interface`
- `show power-inline`
- `show power-inline interface`
show power-inline interface

**Overview**  This command displays a summary of Power over Ethernet (PoE) information for specified ports. If no ports are specified then PoE information is displayed for all ports on the Power Sourcing Equipment (PSE).

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show power-inline interface [\(<\text{port-list}>\)]

**Mode**  User Exec and Privileged Exec

**Usage**  To display PoE information for all PoE ports on the PSE, do not specify any ports.

**Example**  To display the PoE port specific information for all PoE ports on the switch, use the following command:

```
awplus# show power-inline interface
```

To display the PoE port specific information for the port range 1.0.1 to 1.0.4, use the following command:

```
awplus# show power-inline interface port1.0.1-port1.0.4
```

**Output**  Figure 14-4:  Example output from the `show power-inline interface` command

```
awplus# show power-inline interface port1.0.1-port1.0.4
Interface  Admin    Pri  Oper     Power Device      Class Max(mW)
port1.0.1  Disabled Low  Disabled     0 n/a         n/a   n/a
port1.0.2  Enabled  High Powered  3840 Desk Phone 1     5000 [U]
port1.0.3  Enabled  Crit Powered  6720 AccessPoint 2     7000 [C]
port1.0.4  Disabled Low  Disabled     0 n/a         n/a   n/a
```

Table 14-3:  Parameters in the `show power-inline interface` command output

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The PoE port(s) in the format <code>portx.y.z</code>, where <code>x</code> is the device number, <code>y</code> is the module number within the device, and <code>z</code> is the PoE port number within the module.</td>
</tr>
<tr>
<td>Admin</td>
<td>The administrative state of PoE on a PoE port, either <code>Enabled</code> or <code>Disabled</code>.</td>
</tr>
</tbody>
</table>
### POWER OVER ETHERNET COMMANDS

**SHOW POWER-INLINE INTERFACE**

**Table 14-3: Parameters in the show power-inline interface command output**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pri</strong></td>
<td>The current PoE priorities for PoE ports on the PSE, as configured from a power-inline priority command:</td>
</tr>
<tr>
<td></td>
<td>• Low displays when the low parameter is issued. The lowest priority for a PoE enabled port (default).</td>
</tr>
<tr>
<td></td>
<td>• High displays when the high parameter is issued. The second highest priority for a PoE enabled port.</td>
</tr>
<tr>
<td></td>
<td>• Crit displays when the critical parameter is issued. The highest priority for a PoE enabled port.</td>
</tr>
<tr>
<td><strong>Oper</strong></td>
<td>The current PSE PoE port state when this command was issued:</td>
</tr>
<tr>
<td></td>
<td>• Powered displays when there is a PD connected and power is being supplied from the PSE.</td>
</tr>
<tr>
<td></td>
<td>• Denied displays when supplying power would make the PSE go over the power budget.</td>
</tr>
<tr>
<td></td>
<td>• Disabled displays when the PoE port is administratively disabled.</td>
</tr>
<tr>
<td></td>
<td>• Off displays when PoE has been disabled for the port.</td>
</tr>
<tr>
<td></td>
<td>• Fault displays when a PSE goes over its power allocation.</td>
</tr>
<tr>
<td><strong>Power</strong></td>
<td>The power consumption in milliwatts (mW) for the PoE port when this command was entered.</td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Class</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Max (mW)</strong></td>
<td>The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port:</td>
</tr>
<tr>
<td></td>
<td>• [U] if the power limit for a port was user configured (with the power-inline max command).</td>
</tr>
<tr>
<td></td>
<td>• [L] if the power limit for a port was supplied by LLDP.</td>
</tr>
<tr>
<td></td>
<td>• [C] if the power limit for a port was supplied by the PD class.</td>
</tr>
</tbody>
</table>

**Related Commands**

- show power-inline
- show power-inline interface detail
show power-inline interface detail

**Overview**
This command displays detailed information for specified Power over Ethernet (PoE) port(s) on the Power Sourcing Equipment (PSE).

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show power-inline interface [port-list] detail
```

**Mode**
User Exec and Privileged Exec

**Usage**
To show detailed PoE information for all ports on the PSE, do not specify any ports.

The power allocated to each port is listed in the `Power allocated` row, and is limited by the maximum power per Powered Device (PD) class, or a user configured power limit.

**Example**
To display detailed PoE port specific information for the port range 1.0.1 to 1.0.2, use the following command:
```
awplus# show power-inline interface port1.0.1-port1.0.2 detail
```

**Output**
Example output from the `show power-inline interface detail` command

```
awplus#show power-inline interface port1.0.1-1.0.2 detail
Interface port1.0.1
  Powered device type: Desk Phone #1
  PoE admin enabled
  Priority Low
  Detection status: Powered
  Current power consumption: 4800 mW
  Power device class: 1
  Power allocated: 5000 mW (from configuration)
  Detection of legacy devices is disabled
  Powered pairs: Data
Interface port1.0.2
  Powered device type: Access Point #3
  PoE admin enabled
  Priority High
  Detection status: Powered
  Current power consumption: 6720 mW
  Power device class: 2
  Power allocated: 7000 mW (from powered device class)
  Detection of legacy devices is enabled
  Powered pairs: Data
```
## Table 14-4: Parameters in `show power-inline interface detail` command output

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The PoE port(s) in the format <code>portx.y.z</code>, where <code>x</code> is the device number, <code>y</code> is the module number within the device, and <code>z</code> is the PoE port number within the module.</td>
</tr>
<tr>
<td>Powered device type:</td>
<td>The name of the PD, if connected and if power is being supplied to the PD from the PSE, configured with the <code>power-inline description</code> command. <code>n/a</code> displays if a description has not been configured for the PD.</td>
</tr>
<tr>
<td>PoE admin</td>
<td>The administrative state of PoE on a PoE capable port, either <code>Enabled</code> or <code>Disabled</code> as configured from the <code>power-inline enable</code> command or the <code>no power-inline enable</code> command respectively.</td>
</tr>
<tr>
<td>Priority</td>
<td>The PoE priority of a port, which is either <code>Low</code>, <code>High</code>, or <code>Critical</code>, as configured by the <code>power-inline priority</code> command.</td>
</tr>
<tr>
<td>Detection status:</td>
<td>The current PSE PoE port state when this command was issued:</td>
</tr>
<tr>
<td></td>
<td>• <code>Powered</code> displays when there is a PD connected and power is being supplied from the PSE.</td>
</tr>
<tr>
<td></td>
<td>• <code>Denied</code> displays when supplying power would make the PSE go over the power budget.</td>
</tr>
<tr>
<td></td>
<td>• <code>Disabled</code> displays when the PoE port is administratively disabled.</td>
</tr>
<tr>
<td></td>
<td>• <code>Off</code> displays when PoE has been disabled for the port.</td>
</tr>
<tr>
<td></td>
<td>• <code>Fault</code> displays when a PSE goes over its power allocation.</td>
</tr>
<tr>
<td>Current power consumption:</td>
<td>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.</td>
</tr>
<tr>
<td>Powered device class:</td>
<td>The class of the connected PD if connected, and if power is being supplied to the PD from the PSE.</td>
</tr>
<tr>
<td></td>
<td>See the Power over Ethernet (PoE) Feature Overview and Configuration Guide for further information about power classes.</td>
</tr>
<tr>
<td>Power allocated:</td>
<td>The power in milliwatts (mW) allocated for the PoE port. Additionaly, note the following as displayed per PoE port:</td>
</tr>
<tr>
<td></td>
<td>• <code>[U]</code> if the power limit for a port was user configured (with the <code>power-inline max</code> command).</td>
</tr>
<tr>
<td></td>
<td>• <code>[L]</code> if the power limit for a port was supplied by LLDP.</td>
</tr>
<tr>
<td></td>
<td>• <code>[C]</code> if the power limit for a port was supplied by the PD class.</td>
</tr>
</tbody>
</table>
### POWER OVER ETHERNET COMMANDS

#### SHOW POWER-INLINE INTERFACE DETAIL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection of legacy devices is</td>
<td>[Enabled</td>
</tr>
<tr>
<td>Powered pairs:</td>
<td>[Data</td>
</tr>
</tbody>
</table>

### Related Commands
- show power-inline
- show power-inline interface

---

**Table 14-4: Parameters in show power-inline interface detail command output**
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 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.

• VCStack is not supported by the current AlliedWare Plus GVRP implementation.

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 620
- “debug gvrp” on page 621
- “gvrp (interface)” on page 623
- “gvrp dynamic-vlan-creation” on page 624
- “gvrp enable (global)” on page 625
- “gvrp registration” on page 626
- “gvrp timer” on page 627
- “show debugging gvrp” on page 629
- “show gvrp configuration” on page 630
- “show gvrp machine” on page 631
- “show gvrp statistics” on page 632
- “show gvrp timer” on page 633
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>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specify all switchports to clear GVRP statistics.</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>Specify the switchport to clear GVRP statistics.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Usage**
Use this command together with the show gvrp statistics command to troubleshoot GVRP.

**Examples**
To clear all GVRP statistics for all switchport on the switch, enter the command:

```
awplus# clear gvrp statistics all
```

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 | Specifies 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**

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 COMMANDS
GVRP DYNAMIC-VLAN-CREATION

**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**  
```plaintext
gvrp dynamic-vlan-creation  
no gvrp dynamic-vlan-creation
```

**Mode**  Global Configuration

**Default**  Disabled by default.

**Usage**  
You must enable GVRP on both ends of a link for GVRP to propagate VLANs between links.

You must also enable GVRP globally in Global Configuration mode before enabling GVRP on an interface in Interface Configuration mode. Both of these tasks must occur to create VLANs.

**NOTE:** There is limit of 400 VLANs supported by the AlliedWare Plus GVRP implementation. VLANs may be numbered 1-4094, but a limit of 400 of these VLANs are supported.

**Examples**  Enter the following commands for switches with hostnames `switch1` and `switch2` respectively, so `switch1` propagates VLANs to `switch2` and `switch2` propagates VLANs to `switch1`:

**Switch1:**
```
switch1# configure terminal
switch1(config)# gvrp enable
switch1(config)# gvrp dynamic-vlan-creation
```

**Switch2:**
```
switch2# configure terminal
switch2(config)# gvrp enable
switch2(config)# gvrp dynamic-vlan-creation
```

To disable GVRP dynamic VLAN creation on the switch, enter the commands:
```
awplus# configure terminal
awplus(config)# no gvrp dynamic-vlan-creation
```

**Validation Commands**  `show gvrp configuration`

**Related Commands**  `gvrp enable (global)`
gvrp enable (global)

**Overview**  Use this command to enable GVRP globally for the switch. Use the `no` variant of this command to disable GVRP globally for the switch.

**Syntax**
```
gvrp enable
no gvrp enable
```

**Mode**  Global Configuration

**Default**  Disabled by default.

**Usage**  Use this command to enable GVRP on the switch. Note that this command does not enable GVRP on switchports. To enable GVRP on switchports use the `gvrp (interface)` command in Interface Configuration mode. You must issue a `gvrp enable (global)` command before issuing a `gvrp (interface)` command.

You must enable GVRP on both ends of a link for GVRP to propagate VLANs between links.

*NOTE:* MSTP is not supported by the current AlliedWare Plus GVRP implementation. GVRP and MSTP are mutually exclusive. STP and RSTP are supported by GVRP.

Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. GVRP and private VLAN trunk ports are mutually exclusive.

**Examples**  To enable GVRP for the switch, before enabling GVRP on switchports, enter the commands:
```
awplus# configure terminal
awplus(config)# gvrp enable
```

To disable GVRP on the switch, which will also disable GVRP enabled on switchports, enter the commands:
```
awplus# configure terminal
awplus(config)# no gvrp enable
```

**Validation Commands**
```
show gvrp configuration
```

**Related Commands**
```
gvrp (interface)
gvrp dynamic-vlan-creation
```
**GVRP Commands**

**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}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>Specify dynamic GVRP registration and deregistration of VLANs.</td>
</tr>
<tr>
<td>fixed</td>
<td>Specify fixed GVRP registration and deregistration of VLANs.</td>
</tr>
<tr>
<td>forbidden</td>
<td>Specify no GVRP registration of VLANs. VLANs are deregistered.</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration

**Default**
Normal registration is the default.

**Usage**
Configuring a trunk port in normal registration mode allows dynamic creation of VLANs. Normal mode is the default mode. Validate using the `show gvrp configuration` command.

Configuring a trunk port in fixed registration mode allows manual creation of VLANs.

Configuring a trunk port in forbidden registration mode prevents VLAN creation on the port.

**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**
```plaintext
gvrp timer {join <timer-value>|leave <timer-value>|leaveall <timer-value>}

no gvrp timer {join|leave|leaveall}
```

**Mode**
Interface Configuration

**Defaults**
The default join time value is 20 centiseconds (200 milliseconds), the default leave timer value is 60 centiseconds (600 milliseconds), and the default leaveall timer value is 1000 centiseconds (10,000 milliseconds).

**Usage**
When configuring the `leave` timer, set it to more than or equal to three times the `join` timer value. The settings for the `leave` and `join` timers must be the same for all GVRP enabled switches. See also the section “Setting the GVRP Timers” in the GVRP Feature Overview and Configuration Guide.

Use the `show gvrp timer` command to confirm GVRP timers set with this command.

**Examples**
To set the GVRP `join` timer to 30 hundredths of a second (300 milliseconds) for interface `port1.0.1`, enter the commands:
```plaintext
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:
```plaintext
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 display the GVRP debugging option set.
For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
```
show debugging gvrp
```

**Mode**  User Exec and Privileged Exec

**Example**  Enter the following commands to display GVRP debugging output on the console:
```
awplus# configure terminal
awplus(config)# debug gvrp all
awplus(config)# exit
awplus# show debugging gvrp
```

**Output**  See sample output from the `show debugging gvrp` command after entering `debug gvrp all`:

```
GVRP debugging status:
  GVRP Event debugging is on
  GVRP CLI debugging is on
  GVRP Timer debugging is on
  GVRP Packet debugging is on
```

**Related Commands**  `debug gvrp`
show gvrp configuration

**Overview**  
Use this command to display GVRP configuration data for a switch.  
For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show gvrp configuration

**Mode**  
User Exec and Privileged Exec

**Example**  
To show GVRP configuration for the switch, enter the command:

```
awplus# show gvrp configuration
```

**Output**  
The following is an output of this command displaying the GVRP configuration for a switch:

```
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show gvrp machine

**Mode**  User Exec and Privileged Exec

**Example**  To show the GVRP state machine for the switch, enter the command:

```
awplus# show gvrp machine
```

**Output**  See the following output of this command displaying the GVRP state machine.

```
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**

```
show gvrp statistics [<interface>]
```

**Mode**
User Exec and Privileged Exec

**Usage**
Use this command together with the `clear gvrp statistics` command to troubleshoot GVRP.

**Examples**
To show the GVRP statistics for all switchport interfaces, enter the command:

```
awplus# show gvrp statistics
```

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`

<table>
<thead>
<tr>
<th>Port</th>
<th>JoinEmpty</th>
<th>JoinIn</th>
<th>LeaveEmpty</th>
<th>LeaveIn</th>
<th>Empty</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.1</td>
<td>RX 0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>TX 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.0.2</td>
<td>RX 0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>TX 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

**Related Commands**
clear gvrp statistics
**show gvrp timer**

**Overview**  Use this command to display data for the GVRP timers set with the `gvrp timer` command.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  `show gvrp timer <interface>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>The name of the switchport interface.</td>
</tr>
</tbody>
</table>

**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
```
Introduction

Overview  This chapter provides an alphabetical reference of commands used to configure the following protocols:

• Address Resolution Protocol (ARP)
• Domain Name Service (DNS)

For more information, see the IP Feature Overview and Configuration Guide.
Command List

- “arp-aging-timeout” on page 636
- “arp-mac-disparity” on page 637
- “arp (IP address MAC)” on page 638
- “arp log” on page 639
- “arp opportunistic-nd” on page 642
- “clear arp-cache” on page 643
- “clear ip dns forwarding cache” on page 644
- “debug ip dns forwarding” on page 645
- “debug ip packet interface” on page 646
- “ip address” on page 648
- “ip directed-broadcast” on page 650
- “ip dns forwarding” on page 652
- “ip dns forwarding cache” on page 653
- “ip dns forwarding dead-time” on page 654
- “ip dns forwarding retry” on page 655
- “ip dns forwarding source-interface” on page 656
- “ip dns forwarding timeout” on page 657
- “ip domain-list” on page 658
- “ip domain-lookup” on page 659
- “ip domain-name” on page 660
- “ip forward-protocol udp” on page 661
- “ip gratuitous-arp-link” on page 663
- “ip helper-address” on page 665
- “ip local-proxy-arp” on page 667
- “ip name-server” on page 668
- “ip proxy-arp” on page 669
- “ip redirects” on page 670
- “optimistic-nd” on page 671
- “ping” on page 672
- “show arp” on page 673
- “show debugging ip dns forwarding” on page 675
- “show debugging ip packet” on page 676
- “show hosts” on page 678
- “show ip dns forwarding” on page 679
- “show ip dns forwarding cache” on page 680
IP ADDRESSING AND PROTOCOL COMMANDS

- “show ip dns forwarding server” on page 681
- “show ip domain-list” on page 682
- “show ip domain-name” on page 683
- “show ip interface” on page 684
- “show ip name-server” on page 685
- “show ip sockets” on page 686
- “show ip traffic” on page 689
- “tcpdump” on page 695
- “traceroute” on page 696
- “undebug ip packet interface” on page 697
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-432000&gt;</td>
<td>The timeout period in seconds.</td>
</tr>
</tbody>
</table>

**Default**
300 seconds (5 minutes)

**Mode**
Interface Configuration for a VLAN interface.

**Example**
To set the ARP entries on interface vlan30 to time out after two minutes, use the commands:
```
awplus(config)# interface vlan30
awplus(config-if)# arp-aging-timeout 120
```

**Related Commands**
clear arp-cache
show arp
arp-mac-disparity

**Overview**
Use this command in Interface Configuration mode for a VLAN interface to enable the reception of ARP packets that contain a multicast MAC address in the sender field.

By default, ARP packets that contain a multicast MAC address in the sender field are dropped. The `no` variant of this command reverts to the default behavior.

**Syntax**
```
arp-mac-disparity
no arp-mac-disparity
```

**Default**
ARP disparity is disabled. ARP packets with a multicast MAC address in the sender field are dropped.

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
Normally, it is invalid for an ARP request to resolve a multicast MAC address. By default, ARP replies with a multicast MAC addresses are not learned. This command allows control over the learning of dynamic ARPs that resolve to a multicast MAC address.

ARP-MAC disparity may need to be enabled to support multicast network load balancing. The `arp-mac-disparity` command allows ARP replies quoting multicast MAC addresses to be accepted and learned. No `arp-mac-disparity` command reverts to default behavior.

If the ARP-MAC disparity feature is enabled, then the device sends traffic to a single port as specified by the ARP entry.

**Examples**
To enable ARP MAC disparity on interface `vlan2`, use the following commands:
```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp-mac-disparity
```

To disable ARP MAC disparity on interface `vlan2`, use the following commands:
```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no arp-mac-disparity
```

**Related Commands**
- `clear arp-cache`
- `show arp`
arp (IP address MAC)

**Overview**
This command adds a static ARP entry to the ARP cache. This is typically used to add entries for hosts that do not support ARP or to speed up the address resolution function for a host. The ARP entry must not already exist. Use the `alias` parameter to allow your device to respond to ARP requests for this IP address.

The `no` variant of this command removes the static ARP entry. Use the `clear arp-cache` command to remove the dynamic ARP entries in the ARP cache.

**Syntax**
```
arp <ip-addr> <mac-address> [port-number] [alias]
no arp <ip-addr>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>IPv4 address of the device you are adding as a static ARP entry.</td>
</tr>
<tr>
<td><code>&lt;mac-address&gt;</code></td>
<td>MAC address of the device you are adding as a static ARP entry, in hexadecimal notation with the format HHHH.HHHH.HHHH.</td>
</tr>
<tr>
<td><code>&lt;port-number&gt;</code></td>
<td>The port number associated with the IP address. Specify this when the IP address is part of a VLAN.</td>
</tr>
<tr>
<td><code>alias</code></td>
<td>Allows your device to respond to ARP requests for the IP address. Proxy ARP must be enabled on the interface before using this parameter.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Examples**
To add the IP address 10.10.10.9 with the MAC address 0010.2533.4655 into the ARP cache, and have your device respond to ARP requests for this address, use the commands:
```
awplus# configure terminal
awplus(config)# arp 10.10.10.9 0010.2355.4566 alias
```

**Related Commands**
clear arp-cache
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 default hexadecimal notation (HHHH.HHHH.HHHH), or using the IEEE standard hexadecimal notation (HH-HH-HH-HH-HH-HH).

Use the **no** variant of this command to disable the logging of dynamic and static ARP entries in the ARP cache.

**Syntax**

```plaintext
arp log [mac-address-format ieee]
no arp log [mac-address-format ieee]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address-format ieee</td>
<td>Display the MAC address in hexadecimal notation with the standard IEEE format (HH-HH-HH-HH-HH-HH), instead of displaying the MAC address with the default hexadecimal format (HHHH.HHHH.HHHH).</td>
</tr>
</tbody>
</table>

**Default**  
The ARP logging feature is disabled by default.

**Mode**  
Global Configuration

**Usage**  
You have the option to change how the MAC address is displayed in the ARP log message, to use the default hexadecimal notation (HHHH.HHHH.HHHH), or the IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH) when you apply the **mac-address-format ieee** parameter.

Enter the **arp log** command without the optional **mac-address-format ieee** parameter specified for MAC addresses in the ARP log output to use the default hexadecimal notation (HHHH.HHHH.HHHH).

Enter the **arp log mac-address-format ieee** command for MAC addresses in the ARP log output to use the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH).

Use the **no** variant of this command (**no arp log**) without the optional **mac-address-format ieee** parameter specified to disable ARP logging on the device.

Use the **no** variant of this command with the optional **mac-address-format ieee** parameter specified (**no arp log mac-address-format ieee**) to disable IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) and revert to the default hexadecimal notation (HHHH.HHHH.HHHH) for MAC addresses in the ARP log output.

To display ARP log messages use the **show log | include ARP_LOG** command.
**Examples**

To enable ARP logging and use the default hexadecimal notation (HHHH.HHHH.HHHH), use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# arp log
```

To disable ARP logging on the device of MAC addresses displayed using the default hexadecimal notation (HHHH.HHHH.HHHH), use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# no arp log
```

To enable ARP logging and to specify that the MAC address in the log message is displayed in the standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH), use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# arp log mac-address-format ieee
```

To disable ARP logging on the device of MAC addresses displayed using the standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH), and revert to the use of the default hexadecimal notation (HHHH.HHHH.HHHH) instead, use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# no arp log mac-address-format ieee
```

To display ARP log messages, use following command:

```plaintext
awplus# show log | include ARP_LOG
```

**Output**

Below is example output from the `show log | include ARP_LOG` command after enabling ARP logging displaying default hexadecimal notation MAC addresses (HHHH.HHHH.HHHH) using the `arp log` command.

```
awplus#configure terminal
awplus(config)#arp log
awplus(config)#exit
awplus#show log | include ARP_LOG
2010 Apr  6 06:21:01 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add 0013.4078.3b98 (192.168.2.4)
2010 Apr  6 06:22:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 0013.4078.3b98 (192.168.2.4)
2010 Apr  6 06:23:26 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add 0030.940e.136b (192.168.2.20)
2010 Apr  6 06:23:30 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Below is example output from the `show log | include ARP_LOG` command after enabling ARP logging displaying IEEE standard format hexadecimal notation MAC addresses (HH-HH-HH-HH-HH-HH) using the `arp log mac-address format ieee` command.

```
awplus(config)#arp log mac-address-format ieee
```
Table 16-1: Example output from the `show log | include ARP_LOG` command

```
awplus#configure terminal
awplus(config)#arp log mac-address-format ieee
awplus(config)#exit
awplus#show log | include ARP_LOG
2010 Apr  6 06:25:28 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add 00-17-9a-b6-03-69 (192.168.2.12)
2010 Apr  6 06:25:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add 00-03-37-6b-a6-a5 (192.168.2.10)
2010 Apr  6 06:26:53 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-30-94-0e-13-6b (192.168.2.20)
2010 Apr  6 06:27:31 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-17-9a-b6-03-69 (192.168.2.12)
2010 Apr  6 06:28:09 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-03-37-6b-a6-a5 (192.168.2.10)
2010 Apr  6 06:28:14 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Below are the parameters in output of the `show log | include ARP_LOG` command with an ARP log message format of `<ARP_LOG> <port number> <VLAN ID> <Operation> <MAC> <IP> after <date> <time> <severity> <hostname> <program-name> information.`

Table 16-2: Parameters in output of the `show log | include ARP_LOG` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ARP_LOG&gt;</code></td>
<td>Indicates ARP log entry information follows <code>&lt;date&gt; &lt;time&gt; &lt;severity&gt; &lt;hostname&gt; &lt;program name&gt; log information.</code></td>
</tr>
<tr>
<td><code>&lt;port number&gt;</code></td>
<td>Indicates device port number for the ARP log entry.</td>
</tr>
<tr>
<td><code>&lt;VLAN ID&gt;</code></td>
<td>Indicates the VLAN ID for the ARP log entry.</td>
</tr>
<tr>
<td><code>&lt;Operation&gt;</code></td>
<td>Indicates ‘add’ if the ARP log entry displays an ARP addition. Indicates ‘del’ if the ARP log entry displays an ARP deletion.</td>
</tr>
<tr>
<td><code>&lt;MAC&gt;</code></td>
<td>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 <code>arp log</code> or the <code>arp log mac-address-format ieee</code> command.</td>
</tr>
<tr>
<td><code>&lt;IP&gt;</code></td>
<td>Indicates the IP address for the ARP log entry.</td>
</tr>
</tbody>
</table>

**Validation Commands**
- `show running-config`

**Related Commands**
- `show log`
### arp opportunistic-nd

**Overview**  
This command changes the behavior for unsolicited ARP packet forwarding on the device.

Use this command to enable opportunistic neighbor discovery for the global ARP cache.

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**  
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.

Note this command enables or disables opportunistic neighbor discovery for a VRF lite instance if the `VRF lite` parameter and an instance name are applied. If a VRF lite instance is not specified, then opportunistic neighbor discovery is enabled or disabled for device ports configured for IPv4.

**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`

**Validation Commands**

- `show running-config interface`
clear arp-cache

**Overview**  This command deletes dynamic ARP entries from the ARP cache. You can optionally specify the IPv4 address of an ARP entry to be cleared from the ARP cache.

**Syntax**  clear arp-cache [<ip-address>]

**Mode**  Privileged Exec

**Usage**  To display the entries in the ARP cache, use the show arp command. To remove static ARP entries, use the no variant of the arp (IP address MAC) command.

**Example**  To clear all dynamic ARP entries, use the command:

```
awplus# clear arp-cache
```

To clear all dynamic ARP entries associated with the IPv4 address 192.168.1.1, use the command:

```
awplus# clear arp-cache 192.168.1.1
```

**Related Commands**  
- arp-mac-disparity
- arp (IP address MAC)
- show arp
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`
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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>Specify a single Layer 3 interface name (not a range of interfaces)</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Specify all Layer 3 interfaces on the device.</td>
</tr>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>Specify an IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><code>verbose</code></td>
<td>Specify <code>verbose</code> to output more of the IP packet.</td>
</tr>
<tr>
<td></td>
<td>If this keyword is specified then more of the packet is shown in the output.</td>
</tr>
<tr>
<td><code>hex</code></td>
<td>Specify <code>hex</code> to output the IP packet in hexadecimal.</td>
</tr>
<tr>
<td></td>
<td>If this keyword is specified, then the output for the packet is shown in hex.</td>
</tr>
<tr>
<td><code>arp</code></td>
<td>Specify <code>arp</code> to output ARP protocol packets.</td>
</tr>
<tr>
<td></td>
<td>If this keyword is specified, then ARP packets are shown in the output.</td>
</tr>
<tr>
<td><code>udp</code></td>
<td>Specify <code>udp</code> to output UDP protocol packets.</td>
</tr>
<tr>
<td></td>
<td>If this keyword is specified, then UDP packets are shown in the output.</td>
</tr>
<tr>
<td><code>tcp</code></td>
<td>Specify <code>tcp</code> to output TCP protocol packets.</td>
</tr>
<tr>
<td></td>
<td>If this keyword is specified, then TCP packets are shown in the output.</td>
</tr>
<tr>
<td><code>icmp</code></td>
<td>Specify <code>icmp</code> to output ICMP protocol packets.</td>
</tr>
<tr>
<td></td>
<td>If this keyword is specified, then ICMP packets are shown in the output.</td>
</tr>
</tbody>
</table>

**Mode**

Privileged Exec and Global Configuration
**Examples**

To turn on ARP packet debugging on VLAN1, use the command:

```
awplus# debug ip packet interface vlan1 arp
```

To turn on all packet debugging on all interfaces on the device, use the command:

```
awplus# debug ip packet interface all
```

To turn on TCP packet debugging on VLAN1 and IP address 192.168.2.4, use the command:

```
awplus# debug ip packet interface vlan1 address 192.168.2.4 tcp
```

To turn off IP packet interface debugging on all interfaces, use the command:

```
awplus# no debug ip packet interface
```

To turn off IP packet interface debugging on interface VLAN2, use the command:

```
awplus# no debug ip packet interface vlan2
```

**Related Commands**

- `no debug all`
- `show debugging ip dns forwarding`
- `tcpdump`
- `terminal monitor`
- `undebug ip packet interface`
IP ADDRESSING AND PROTOCOL COMMANDS

ip address

Overview
This command sets a static IP address on an interface. To set the primary IP address on the interface, specify only `ip address <ip-address/m>`. This overwrites any configured primary IP address. To add additional IP addresses on this interface, use the `secondary` parameter. You must configure a primary address on the interface before configuring a secondary address.

**NOTE:** Use `show running-config` interface not `show ip interface brief` when you need to view a secondary address configured on an interface. `show ip interface brief` will only show the primary address not a secondary address for an interface.

The no variant of this command removes the IP address from the interface. You cannot remove the primary address when a secondary address is present.

Syntax
```
ip address <ip-addr/prefix-length> [secondary] [label <label>]  
no ip address <ip-addr/prefix-length> [secondary]  
no ip address
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-addr/prefix-length&gt;</code></td>
<td>The IPv4 address and prefix length you are assigning to the interface.</td>
</tr>
<tr>
<td>secondary</td>
<td>Secondary IP address.</td>
</tr>
<tr>
<td>label</td>
<td>Adds a user-defined description of the secondary IP address.</td>
</tr>
<tr>
<td><code>&lt;label&gt;</code></td>
<td>A user-defined description of the secondary IP address. Valid characters are any printable character and spaces.</td>
</tr>
</tbody>
</table>

Mode
Interface Configuration for a VLAN interface or a local loopback interface.

Examples
To add the primary IP address 10.10.10.50/24 to the interface vlan3, use the following commands:
```
awplus# configure terminal  
awplus(config)# interface vlan3  
awplus(config-if)# ip address 10.10.10.50/24
```

To add the secondary IP address 10.10.11.50/24 to the same interface, use the following commands:
```
awplus# configure terminal  
awplus(config)# interface vlan3  
awplus(config-if)# ip address 10.10.11.50/24 secondary
```
To add the IP address 10.10.11.50/24 to the local loopback interface lo, use the following commands:

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.11.50/24
```

**Related Commands**
- `interface (to configure)`
- `show ip interface`
- `show running-config interface`
ip 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**  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 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 ip directed-broadcast, to flood broadcast packets out via the vlan2 interface, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip directed-broadcast
```

To disable ip directed-broadcast, disabling 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 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** See the IP Feature Overview and Configuration Guide for more information about DNS Relay. 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 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 <0-1000>] [timeout <60-3600>]
no ip dns forwarding cache [size|timeout]
```

**Default**  The default cache size is 0 (no entries) and the default lifetime is 1800 seconds.

**Mode**  Global Configuration

**Usage**  See the **IP Feature Overview and Configuration Guide** for more information about DNS Relay.

**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`
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;60-43200&gt;</code></td>
<td>Set the DNS forwarding dead-time in seconds. At the dead-time set, the switch stops sending DNS requests to an unresponsive server.</td>
</tr>
</tbody>
</table>

**Default**
The default time to stop sending DNS requests to an unresponsive server is 3600 seconds.

**Mode**
Local Configuration

**Usage**
See the IP Feature Overview and Configuration Guide for more information about DNS Relay. 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**

```plaintext
ip dns forwarding retry <0-100>
no ip dns forwarding retry
```

**Default**  The default number of retries is 2 DNS requests to an unresponsive server.

**Mode**  Global Configuration

**Usage**  See the IP Feature Overview and Configuration Guide for more information about DNS Relay. 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:

```plaintext
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:

```plaintext
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
```

**Default**  The default is that no interface is set and the device selects the appropriate source IP address automatically.

**Mode**  Global Configuration

**Usage**  See the IP Feature Overview and Configuration Guide for more information about DNS Relay.

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-name&gt;</td>
<td>An alphanumeric string that is the interface name.</td>
</tr>
</tbody>
</table>
**ip dns forwarding timeout**

**Overview**
Use this command to set the time period for the DNS Relay to wait for a DNS response.

Use the `no` variant of this command to set the time period to wait for a DNS response to the default of 3 seconds.

**Syntax**
```
ip dns forwarding timeout <0-3600>
no ip dns forwarding timeout
```

**Default**
The default timeout value is 3 seconds.

**Mode**
Global Configuration

**Usage**
See the IP Feature Overview and Configuration Guide for more information about DNS Relay.

**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. Domain are appended to incomplete host names in DNS requests. Each domain in this list is tried in turn in DNS lookups. This list is ordered so that the first entry you create is checked first.

The **no** variant of this command deletes a domain from the list.

**Syntax**  

```
ip domain-list <domain-name>
no ip domain-list <domain-name>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;domain-name&gt;</code></td>
<td>Domain string, for example “company.com”.</td>
</tr>
</tbody>
</table>

**Mode**  Global Configuration

**Usage**  If there are no domains in the DNS list, then your device uses the domain specified with the **ip domain-name** command. If any domain exists in the DNS list, then the device does not use the domain set using the **ip domain-name** command.

**Example**  To add the domain **example.net** to the DNS list, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-list example.net
```

**Related Commands**  
- **ip domain-lookup**
- **ip domain-name**
- **show ip domain-list**
ip domain-lookup

**Overview**
This command enables the DNS client on your device. This allows you to use domain names instead of IP addresses in commands. The DNS client resolves the domain name into an IP address by sending a DNS inquiry to a DNS server, specified with the `ip name-server` command.

The **no** variant of this command disables the DNS client. The client will not attempt to resolve domain names. You must use IP addresses to specify hosts in commands.

**Syntax**
```
ip domain-lookup
no ip domain-lookup
```

**Mode**
Global Configuration

**Usage**
The client is enabled by default. However, it does not attempt DNS inquiries unless there is a DNS server configured.

For more information about DNS clients, see the IP Feature Overview and Configuration Guide.

**Examples**
To enable the DNS client on your device, use the following commands:
```
awplus# configure terminal
awplus(config)# ip domain-lookup
```
To disable the DNS client on your device, use the following commands:
```
awplus# configure terminal
awplus(config)# no ip domain-lookup
```

**Related Commands**
- `ip domain-list`
- `ip domain-name`
- `ip name-server`
- `show hosts`
- `show ip name-server`
ip domain-name

**Overview**
This command sets a default domain for the DNS. The DNS client appends this domain to incomplete host-names in DNS requests.

The `no` variant of this command removes the domain-name previously set by this command.

**Syntax**

```
ip domain-name <domain-name>
no ip domain-name <domain-name>
```

**Mode**
Global Configuration

**Usage**
If there are no domains in the DNS list (created using the `ip domain-list` command) then your device uses the domain specified with this command. If any domain exists in the DNS list, then the device does not use the domain configured with this command.

When your device is using its DHCP client for an interface, it can receive Option 15 from the DHCP server. This option replaces the domain name set with this command.

**Example**
To configure the domain name, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-name company.com
```

**Related Commands**
ip domain-list
show ip domain-list
show ip domain-name

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;domain-name&gt;</td>
<td>Domain string, for example &quot;company.com&quot;.</td>
</tr>
</tbody>
</table>
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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>UDP Port Number.</td>
</tr>
</tbody>
</table>

Default
The `ip forward-protocol udp` command is not enabled by default.

Mode
Global Configuration

Usage
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.

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>
```

**Validation Commands**
- `show running-config`

**Related Commands**
- `ip helper-address`
- `ip directed-broadcast`
IP GRATUITOUS-ARP-LINK

Overview
This command sets the Gratuitous ARP time limit for all switchports. The time limit restricts the sending of Gratuitous ARP packets to one Gratuitous ARP packet within the time in seconds.

NOTE: This command specifies time between sequences of Gratuitous ARP packets, and time between individual Gratuitous ARP packets occurring in a sequence, to allow legacy support for older devices and interoperation 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-300&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

Default
The default Gratuitous ARP time limit for all switchports is 8 seconds.

Mode
Global Configuration

Usage
Every switchport will send a sequence of 3 Gratuitous ARP packets to each VLAN that the switchport is a member of, whenever the switchport moves to the forwarding state. The first Gratuitous ARP packet is sent 1 second after the switchport becomes a forwarding switchport. The second and third Gratuitous ARP packets are each sent after the time period specified by the Gratuitous ARP time limit.

Additionally, the Gratuitous ARP time limit specifies the minimum time between the end of one Gratuitous ARP sequence and the start of another Gratuitous ARP sequence. When a link is flapping, the switchport’s state is set to forwarding several times. The Gratuitous ARP time limit is imposed to prevent Gratuitous ARP packets from being sent undesirably often.

Examples
To disable the sending of Gratuitous ARP packets, use the commands:

awplus# configure terminal
awplus(config)# ip gratuitous-arp-link 0
To restrict the sending of Gratuitous ARP packets to one every 20 seconds, use the commands:

```plaintext
awplus# configure terminal
awplus(config)# ip gratuitous-arp-link 20
```

**Validation Commands**

```
show running-config
```
ip helper-address

**Overview**  
This command adds 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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>Forwarding destination IP address for IP Helper.</td>
</tr>
</tbody>
</table>

**Default**  
The destination address for the **ip helper-address** command is not configured by default.

**Mode**  
Interface Configuration for a VLAN interface or a local loopback interface.

**Usage**  
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.

**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.

The **ip helper-address** 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** command.

See the IP Feature Overview and Configuration Guide for more information about DNS 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
```

**Validation Commands**

show running-config

**Related Commands**

ip forward-protocol udp

ip directed-broadcast
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 a VLAN interface or a local loopback interface.

**Examples**
To enable your device to apply Local Proxy ARP on the interface `vlan7`, use the following commands:
```
awplus# configure terminal
awplus(config)# interface vlan7
awplus(config-if)# ip local-proxy-arp
```

To disable your device to apply Local Proxy ARP on the interface `vlan7`, use the following commands:
```
awplus# configure terminal
awplus(config)# interface vlan7
awplus(config-if)# no ip local-proxy-arp
```

**Related Commands**
- `ip proxy-arp`
- `show arp`
- `show running-config`
**ip name-server**

**Overview**  
This command adds IPv4 or IPv6 DNS server addresses. The DNS client on your device sends DNS queries to IP addresses in this list when trying to resolve a host name. Host names cannot be resolved until you have added at least one server to this list. A maximum of three name servers can be added to this list.

The **no** variant of this command removes the specified DNS name-server address.

**Syntax**  
```
ip name-server <ip-addr>
no ip name-server <ip-addr>
```  

**Mode**  
Global Configuration

**Usage**  
When your device is using its DHCP client for an interface, it can receive Option 6 messages from the DHCP server. This option appends the name server list with more DNS servers.

For more information about DHCP and DNS, see the *IP Feature Overview and Configuration Guide*.

**Examples**  
To allow a device to send DNS queries to a DNS server with the IPv4 address 10.10.10.5, use the commands:
```
awplus# configure terminal
awplus(config)# ip name-server 10.10.10.5
```

To enable your device to send DNS queries to a DNS server with the IPv6 address 2001:0db8:010d::1, use the commands:
```
awplus# configure terminal
awplus(config)# ip name-server 2001:0db8:010d::1
```

**Related Commands**  
ip domain-list
ip domain-lookup
ip domain-name
show ip dns forwarding cache
show ip name-server
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 a VLAN interface or a local loopback interface.

**Examples**

To enable your device to Proxy ARP on the interface `vlan13`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan13
awplus(config-if)# ip proxy-arp
```

To disable your device to Proxy ARP on the interface `vlan13`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan13
awplus(config-if)# no ip proxy-arp
```

**Related Commands**

- `arp (IP address MAC)`
- `ip local-proxy-arp`
- `show arp`
- `show running-config`
**ip redirects**

**Overview**  
This command enables ICMP redirects for an interface.  
Use the **no** variant of this command to disable the sending of ICMP redirects for an interface.

This command enables ICMP redirects for a device.  
Use the **no** variant of this command to disable the sending of ICMP redirects for a device.

**Syntax**  
`ip redirects`  
`no ip redirects`

**Default**  
ICMP redirects are disabled by default.

**Mode**  
Global Configuration

**Usage**  
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 also used when the subnet or network of the source address is on the same subnet or network as the next-hop address for a packet.

Use the **ip redirects** command to allow the sending of ICMP redirects whenever the device receives a packet that is routed on the same interface that the packet was sent on.

Use the **no** variant of this command to disallow the sending of ICMP redirects whenever the device receives a packet that is routed on the same interface that the packet was sent on.

**Examples**  
To enable ICMP redirects, use the following commands:

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

To disable ICMP redirects, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip redirects
```
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**
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 neighbor is put 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 `vlan100`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan100
awplus(config-if)# optimistic-nd
```

To disable the optimistic neighbor discovery feature on `vlan100`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan100
awplus(config-if)# no optimistic-nd
```

**Validation Commands**
`show running-config`
ping

**Overview**  This command sends a query to another IPv4 host (send Echo Request messages).

**Syntax**  
```plaintext
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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;host&gt;</td>
<td>The destination IP address or hostname.</td>
</tr>
<tr>
<td>broadcast</td>
<td>Allow pinging of a broadcast address.</td>
</tr>
<tr>
<td>df-bit</td>
<td>Enable or disable the do-not-fragment bit in the IP header.</td>
</tr>
<tr>
<td>interval &lt;0-128&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>pattern &lt;hex-data-pattern&gt;</td>
<td>Specify the hex data pattern.</td>
</tr>
<tr>
<td>repeat</td>
<td>Specify the number of ping packets to send.</td>
</tr>
<tr>
<td>&lt;1-2147483647&gt;</td>
<td>Specify repeat count. The default is 5.</td>
</tr>
<tr>
<td>continuous</td>
<td>Continuous ping</td>
</tr>
<tr>
<td>size &lt;36-18024&gt;</td>
<td>The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).</td>
</tr>
<tr>
<td>source &lt;ip-addr&gt;</td>
<td>The IP address of a configured IP interface to use as the source in the IP header of the ping packet.</td>
</tr>
<tr>
<td>timeout &lt;1-65535&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>tos &lt;0-255&gt;</td>
<td>The value of the type of service in the IP header.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**  To ping the IP address 10.10.0.5 use the following command:

```
awplus# ping 10.10.0.5
```
**show arp**

**Overview**  Use this command to display entries in the ARP routing and forwarding table—the ARP cache contains mappings of IP addresses to physical addresses for hosts. To have a dynamic entry in the ARP cache, a host must have used the ARP protocol to access another host.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  

```plaintext
show arp [security [interface [<interface-list>]]]
show arp [statistics [detail][interface [<interface-list>]]]
```

**Mode**  User Exec and Privileged Exec

**Usage**  Running this command with no additional parameters will display all entries in the ARP routing and forwarding table.

**Example**  To display all ARP entries in the ARP cache, use the following command:

```
awplus# show arp
```

**Output**  Figure 16-1: Example output from the `show arp` command

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Interface</th>
<th>Port</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.2</td>
<td>0015.77ad.fad8</td>
<td>vlan1</td>
<td>port1.0.1</td>
<td>dynamic</td>
</tr>
<tr>
<td>192.168.20.2</td>
<td>0015.77ad.fa48</td>
<td>vlan2</td>
<td>port1.0.2</td>
<td>dynamic</td>
</tr>
<tr>
<td>192.168.1.100</td>
<td>00d0.6b04.2a42</td>
<td>vlan2</td>
<td>port1.0.6</td>
<td>static</td>
</tr>
</tbody>
</table>

Table 16-3: Parameters in the output of the `show arp` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the network device this entry maps to.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Hardware address of the network device.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface over which the network device is accessed.</td>
</tr>
<tr>
<td>Port</td>
<td>Physical port that the network device is attached to.</td>
</tr>
<tr>
<td>Type</td>
<td>Whether the entry is a static or dynamic entry. Static entries are added using the <code>arp (IP address MAC)</code> command. Dynamic entries are learned from ARP request/reply message exchanges.</td>
</tr>
</tbody>
</table>
Related Commands

arp (IP address MAC)
clear arp-cache
**show debugging ip dns forwarding**

**Overview**  
Use this command to display the DNS Relay debugging status. DNS Relay debugging is set using the `debug ip dns forwarding` command.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
`show debugging ip 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 16-2: Example output from the `show debugging ip dns forwarding` command

```
awplus# show debugging ip dns forwarding
DNS Relay debugging status:
  debugging is on
```

**Related Commands**  
`debug ip dns forwarding`
**show debugging ip packet**

**Overview**  Use this command to show the IP interface debugging status. IP interface debugging is set using the `debug ip packet interface` command.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  `show debugging ip packet`

**Mode**  User Exec and Privileged Exec

**Example**  To display the IP interface debugging status when the terminal monitor off, use the command:

```bash
awplus# terminal no monitor
awplus# show debug ip packet
```

**Output**  Figure 16-3: Example output from the `show debugging ip packet` command with terminal monitor off

```
awplus#terminal no monitor
awplus#show debug ip packet
IP debugging status:
interface all tcp (stopped)
interface vlan1 arp verbose (stopped)
```

**Example**  To display the IP interface debugging status when the terminal monitor is on, use the command:

```bash
awplus# terminal monitor
awplus# show debug ip packet
```

**Output**  Figure 16-4: Example output from the `show debugging ip packet` command with terminal monitor on

```
awplus#terminal monitor
awplus#show debug ip packet
IP debugging status:
interface all tcp (running)
interface vlan1 arp verbose (running)
```
IP ADDRESSING AND PROTOCOL COMMANDS
SHOW DEBUGGING IP PACKET

**Related Commands**
- debug ip packet interface
- terminal monitor
show hosts

**Overview**  This command shows the default domain, domain list, and name servers configured on your device.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show hosts

**Mode**  User Exec and Privileged Exec

**Example**  To display the default domain, use the command:

```
awplus# show hosts
```

**Output**  Figure 16-5:  Example output from the **show hosts** command

```
awplus#show hosts
Default domain is mycompany.com
Domain list: company.com
Name/address lookup uses domain service
Name servers are 10.10.0.2 10.10.0.88
```

**Related Commands**  
ip domain-list  
ip domain-lookup  
ip domain-name  
ip name-server
show ip 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 16-6:  Example output from the `show ip dns forwarding` command

```
awplus#show ip dns forwarding
Max-Retry : 2
Timeout   : 3 second(s)
Dead-Time : 3600 second(s)
Source-Interface: not specified
DNS Cache : disabled
```

**Related Commands**  ip dns forwarding
show ip dns forwarding cache

Overview  Use this command to display the DNS Relay name resolver cache.

Syntax  show ip dns forwarding cache

Mode  User Exec and Privileged Exec

Example  To display the DNS Relay name resolver cache, use the command:

```
awplus# show ip dns forwarding cache
```

Output  Figure 16-7:  Example output from the show ip dns forwarding cache command

```
awplus# show ip dns forwarding cache

<table>
<thead>
<tr>
<th>Host</th>
<th>Address</th>
<th>Expires</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>172.16.1.1.</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>mail.example.com</td>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>180  CNAME</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>172.16.1.1.</td>
<td>180</td>
<td>REVERSE</td>
</tr>
<tr>
<td>mail.example.com</td>
<td>172.16.1.5.</td>
<td>180</td>
<td></td>
</tr>
</tbody>
</table>
```

Related Commands  ip dns forwarding cache

ip name-server
show ip dns forwarding server

**Overview**

**Syntax**

```
show ip dns forwarding server
```

**Parameter** | **Description**
---|---
forwarding | The DNS forwarding name server.
server

**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 16-8: Example output from the `show ip dns forwarding server` command

```
awplus# show ip dns forwarding server
Servers  | Forwards | Fails | Dead-Time
---------|---------|------|---------
172.16.1.1  | 12      | 0    | active
172.16.1.2  | 6       | 3    | 3900
```

Figure 16-9: :

**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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  `show ip domain-list`

**Mode**  User Exec and Privileged Exec

**Example**  To display the list of domains in the domain list, use the command:

```
awplus# show ip domain-list
```

**Output**  Figure 16-10: Example output from the `show ip domain-list` command

```
awplus# show ip domain-list
alliedtelesis.com
mycompany.com
```

**Related Commands**  `ip domain-list`

`ip domain-lookup`
**show ip domain-name**

**Overview**  This command shows the default domain configured on your device. When there are no entries in the DNS list, the DNS client appends this domain to incomplete hostnames when sending a DNS inquiry to a DNS server.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
```bash
show ip domain-name
```

**Mode**  User Exec and Privileged Exec

**Example**  To display the default domain configured on your device, use the command:

```bash
awplus# show ip domain-name
```

**Output**  Figure 16-11: Example output from the `show ip domain-name` command

```bash
awplus# show ip domain-name
alliedtelesis.com
```

**Related Commands**  
- `ip domain-name`
- `ip domain-lookup`
show ip interface

**Overview**
Use this command to display information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
show ip interface [<interface-list>] [brief]

**Parameter**
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-list&gt;</td>
</tr>
<tr>
<td>• a n i n t e r f a c e , e . g .  v l a n 2</td>
</tr>
<tr>
<td>• a c o n t i n u o u s r a n g e o f i n t e r f a c e s s e p a r a t e d b y a h y p h e n , e . g . v l a n 2 - 8 o r v l a n 2 - v l a n 5</td>
</tr>
<tr>
<td>• a c o m m a - s e p a r a t e d l i s t o f i n t e r f a c e s o r i n t e r f a c e r a n g e s , e . g . v l a n 2 , v l a n 5 , v l a n 8 - 1 0</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Examples**
To show brief information for the assigned IP address for interface port1.0.2 use the command:

```
awplus# show ip interface port1.0.2 brief
```

To show the IP addresses assigned to vlan2 and vlan3, use the command:

```
awplus# show ip interface vlan2-3 brief
```

**Output**
Figure 16-12: Example output from the **show ip interface brief** command

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.2</td>
<td>unassigned</td>
<td>admin up</td>
<td>down</td>
</tr>
<tr>
<td>vlan1</td>
<td>192.168.1.1</td>
<td>admin up</td>
<td>running</td>
</tr>
<tr>
<td>vlan2</td>
<td>192.168.2.1</td>
<td>admin up</td>
<td>running</td>
</tr>
<tr>
<td>vlan3</td>
<td>192.168.3.1</td>
<td>admin up</td>
<td>running</td>
</tr>
<tr>
<td>vlan8</td>
<td>unassigned</td>
<td>admin up</td>
<td>down</td>
</tr>
</tbody>
</table>
show ip name-server

**Overview**  This command displays a list of IPv4 and IPv6 DNS server addresses that your device will send DNS requests to. This is a static list configured using the `ip name-server` command.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show ip name-server

**Mode**  User Exec and Privileged Exec

**Example**  To display the list of DNS servers that your device sends DNS requests to, use the command:

```
awplus# show ip name-server
```

**Output**  Figure 16-13: Example output from the `show ip name-server` command

```
awplus# show ip name-server
10.10.0.123
10.10.0.124
2001:0db8:010d::1
```

**Related Commands**

- ip domain-lookup
- ip name-server
show ip sockets

**Overview**  Use this command to display information about the IP or TCP sockets that are present on the device. It includes TCP, UDP listen sockets, displaying associated IP address and port.

The information displayed for established TCP sessions includes the remote IP address, port, and session state. Raw IP protocol listen socket information is also displayed for protocols such as VRRP and ICMP6, which are configured to receive IP packets with the associated protocol number.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
`show ip sockets`

**Mode**  Privileged Exec

**Usage**  Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

Note that this command does not display sockets that are used internally for exchanging data between the various processes that exist on the device and are involved in its operation and management. It only displays sockets that are present for the purposes of communicating with other external devices.

**Example**  To display ip sockets currently present on the device, use the command:

```
awplus# show ip sockets
```

**Output**  Figure 16-14: Example output from the `show ip sockets` command

<table>
<thead>
<tr>
<th>Socket information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not showing 40 local connections</td>
</tr>
<tr>
<td>Not showing 7 local listening ports</td>
</tr>
<tr>
<td>Typ</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>tcp</td>
</tr>
<tr>
<td>tcp</td>
</tr>
<tr>
<td>tcp</td>
</tr>
<tr>
<td>tcp</td>
</tr>
<tr>
<td>tcp</td>
</tr>
<tr>
<td>tcp</td>
</tr>
<tr>
<td>tcp</td>
</tr>
<tr>
<td>udp</td>
</tr>
<tr>
<td>udp</td>
</tr>
<tr>
<td>udp</td>
</tr>
<tr>
<td>udp</td>
</tr>
<tr>
<td>raw</td>
</tr>
<tr>
<td>raw</td>
</tr>
<tr>
<td>raw</td>
</tr>
</tbody>
</table>
### Table 16-4: Parameters in the output of the `show ip sockets` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not showing &lt;number&gt; local connections</td>
<td>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. &lt;number&gt; is some positive integer.</td>
</tr>
<tr>
<td>Not showing &lt;number&gt; local listening ports</td>
<td>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. &lt;number&gt; is some positive integer.</td>
</tr>
<tr>
<td>Typ</td>
<td>This column displays the type of the socket. Possible values for this column are: &lt;br&gt;tcp: IP Protocol 6  &lt;br&gt;udp: IP Protocol 17  &lt;br&gt;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.</td>
</tr>
<tr>
<td>Local Address</td>
<td>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: <a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a></td>
</tr>
</tbody>
</table>
## Show IP Sockets Command

### Parameters in the output of the `show ip sockets` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Address</td>
<td>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 <code>:</code>. If the socket will accept packets addressed from any IP address, the IP address will be <code>0.0.0.0</code> for IPv4 or <code>::</code> 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 <code>:</code>. 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 <code>0.0.0.0:</code> or <code>::</code> for IPv4 and IPv6, respectively.</td>
</tr>
<tr>
<td>State</td>
<td>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.</td>
</tr>
</tbody>
</table>
**show ip traffic**

**Overview**
Use this command to display statistics regarding IP traffic sent and received by all interfaces on the device, showing totals for IP and IPv6 and then broken down into sub-categories such as TCP, UDP, ICMP and their IPv6 equivalents when appropriate.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
show ip traffic

**Mode**
Privileged Exec

**Example**
To display IP traffic statistics, use the command:

```
awplus# show ip traffic
```

**Output**
Figure 16-15: Example output from the `show ip traffic` command

```
IP:
  261998 packets received
  261998 delivered
  261998 sent
  69721 multicast packets received
  69721 multicast packets sent
  23202841 bytes received
  23202841 bytes sent
  7669296 multicast bytes received
  7669296 multicast bytes sent
IPv6:
  28 packets discarded on transmit due to no route
ICMP6:
UDP6:
UDPLite6:
TCP:
  0 remote connections established
  40 local connections established
  7 remote listening ports
  7 local listening ports
  261 active connection openings
  247 passive connection openings
  14 connection attempts failed
  122535 segments received
  122535 segments transmitted
  14 resets transmitted
  227 TCP sockets finished time wait in fast timer
  155 delayed acks sent
  21187 headers predicted
  736 pure ACKs
  80497 pure ACKs predicted
UDP:
  139468 datagrams received
  139468 datagrams sent
UDPLite:
```
### Table 16-5: Parameters in the output of the `show ip traffic` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv4 counters</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv6 counters</td>
</tr>
<tr>
<td>received packets with no route</td>
<td>Received packets with no route</td>
</tr>
<tr>
<td>truncated packets received</td>
<td>Truncated packets received</td>
</tr>
<tr>
<td>multicast packets received</td>
<td>Multicast packets received</td>
</tr>
<tr>
<td>multicast packets sent</td>
<td>Multicast packets sent</td>
</tr>
<tr>
<td>broadcast packets received</td>
<td>Broadcast packets received</td>
</tr>
<tr>
<td>broadcast packets sent</td>
<td>Broadcast packets sent</td>
</tr>
<tr>
<td>bytes received</td>
<td>Bytes received</td>
</tr>
<tr>
<td>bytes sent</td>
<td>Bytes sent</td>
</tr>
<tr>
<td>multicast bytes received</td>
<td>Multicast bytes received</td>
</tr>
<tr>
<td>multicast bytes sent</td>
<td>Multicast bytes sent</td>
</tr>
<tr>
<td>broadcast bytes received</td>
<td>Broadcast bytes received</td>
</tr>
<tr>
<td>broadcast bytes sent</td>
<td>Broadcast bytes sent</td>
</tr>
<tr>
<td>packets received</td>
<td>Packets received</td>
</tr>
<tr>
<td>packets received with invalid headers</td>
<td>Packets received with invalid headers</td>
</tr>
<tr>
<td>oversize packets received</td>
<td>Oversize packets received</td>
</tr>
<tr>
<td>packets received with no route</td>
<td>Packets received with no route</td>
</tr>
<tr>
<td>packets received with invalid address</td>
<td>Packets received with invalid address</td>
</tr>
<tr>
<td>packets received with unknown protocol</td>
<td>Packets received with unknown protocol</td>
</tr>
<tr>
<td>truncated packets received</td>
<td>Truncated packets received</td>
</tr>
<tr>
<td>received packets discarded</td>
<td>Received packets discarded</td>
</tr>
<tr>
<td>received packets delivered</td>
<td>Received packets delivered</td>
</tr>
<tr>
<td>forwarded packets transmitted</td>
<td>Forwarded packets transmitted</td>
</tr>
<tr>
<td>packets transmitted</td>
<td>Packets transmitted</td>
</tr>
<tr>
<td>packets discarded on transmit</td>
<td>Packets discarded on transmit</td>
</tr>
<tr>
<td>packets discarded on transmit due to no route</td>
<td>Packets discarded on transmit due to no route</td>
</tr>
<tr>
<td>fragment reassembly timeouts</td>
<td>Fragment reassembly timeouts</td>
</tr>
<tr>
<td>fragment reassembly required</td>
<td>Fragment reassembly required</td>
</tr>
<tr>
<td>fragment reassembly OK</td>
<td>Fragment reassembly OK</td>
</tr>
</tbody>
</table>
Table 16-5: Parameters in the output of the `show ip traffic` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fragment reassembly failures</td>
<td>Fragment reassembly failures</td>
</tr>
<tr>
<td>fragmentations succeeded</td>
<td>Fragmentations succeeded</td>
</tr>
<tr>
<td>fragmentations failed</td>
<td>Fragmentations failed</td>
</tr>
<tr>
<td>fragments created</td>
<td>Fragments created</td>
</tr>
<tr>
<td>ICMP6</td>
<td>ICMPv6 counters</td>
</tr>
<tr>
<td>messages received</td>
<td>Messages received</td>
</tr>
<tr>
<td>errors received</td>
<td>Errors received</td>
</tr>
<tr>
<td>messages sent</td>
<td>Messages sent</td>
</tr>
<tr>
<td>TCP</td>
<td>TCP counters</td>
</tr>
<tr>
<td>remote connections established</td>
<td>Remote connections established</td>
</tr>
<tr>
<td>local connections established</td>
<td>Local connections established</td>
</tr>
<tr>
<td>remote listening ports</td>
<td>Remote listening ports</td>
</tr>
<tr>
<td>local listening ports</td>
<td>Local listening ports</td>
</tr>
<tr>
<td>active connection openings</td>
<td>Active connection openings</td>
</tr>
<tr>
<td>passive connection openings</td>
<td>Passive connection openings</td>
</tr>
<tr>
<td>connection attempts failed</td>
<td>Connection attempts failed</td>
</tr>
<tr>
<td>connection resets received</td>
<td>Connection resets received</td>
</tr>
<tr>
<td>segments received</td>
<td>Segments received</td>
</tr>
<tr>
<td>segments transmitted</td>
<td>Segments transmitted</td>
</tr>
<tr>
<td>retransmits</td>
<td>Retransmits</td>
</tr>
<tr>
<td>bad segments received</td>
<td>Bad segments received</td>
</tr>
<tr>
<td>resets transmitted</td>
<td>Resets transmitted</td>
</tr>
<tr>
<td>datagrams received</td>
<td>Datagrams received</td>
</tr>
<tr>
<td>received for unknown port</td>
<td>Received for unknown port</td>
</tr>
<tr>
<td>datagrams sent</td>
<td>Datagrams sent</td>
</tr>
<tr>
<td>syncookies sent</td>
<td>Syncookies sent</td>
</tr>
<tr>
<td>syncookies received</td>
<td>Syncookies received</td>
</tr>
<tr>
<td>syncookies failed</td>
<td>Syncookies failed</td>
</tr>
<tr>
<td>embryonic resets</td>
<td>Embryonic resets</td>
</tr>
<tr>
<td>sockets pruned</td>
<td>Sockets pruned</td>
</tr>
<tr>
<td>ICMPs out of window</td>
<td>ICMPs out of window</td>
</tr>
<tr>
<td>ICMPs dropped due to lock</td>
<td>ICMPs dropped due to lock</td>
</tr>
</tbody>
</table>
Table 16-5: Parameters in the output of the `show ip traffic` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARPs filtered</td>
<td>ARPs filtered</td>
</tr>
<tr>
<td>TCP sockets finished time wait in fast timer</td>
<td>TCP sockets finished time wait in fast timer</td>
</tr>
<tr>
<td>time wait sockets recycled by time stamp</td>
<td>Time wait sockets recycled by time stamp</td>
</tr>
<tr>
<td>time wait sockets killed</td>
<td>Time wait sockets killed</td>
</tr>
<tr>
<td>delayed acks sent</td>
<td>Delayed acks sent</td>
</tr>
<tr>
<td>delayed acks lost</td>
<td>Delayed acks lost</td>
</tr>
<tr>
<td>listening socket overflows</td>
<td>Listening socket overflows</td>
</tr>
<tr>
<td>listening socket drops</td>
<td>Listening socket drops</td>
</tr>
<tr>
<td>headers predicted</td>
<td>Headers predicted</td>
</tr>
<tr>
<td>pure ACKs</td>
<td>Pure ACKs</td>
</tr>
<tr>
<td>pure ACKs predicted</td>
<td>Pure ACKs predicted</td>
</tr>
<tr>
<td>losses recovered by TCP Reno</td>
<td>Losses recovered by TCP Reno</td>
</tr>
<tr>
<td>losses recovered by SACK</td>
<td>Losses recovered by SACK</td>
</tr>
<tr>
<td>SACKs renegged</td>
<td>SACKs renegged</td>
</tr>
<tr>
<td>detected reordering by FACK</td>
<td>Detected reordering by FACK</td>
</tr>
<tr>
<td>detected reordering by SACK</td>
<td>Detected reordering by SACK</td>
</tr>
<tr>
<td>detected reordering by TCP Reno</td>
<td>Detected reordering by TCP Reno</td>
</tr>
<tr>
<td>detected reordering by sequence</td>
<td>Detected reordering by sequence</td>
</tr>
<tr>
<td>full undos</td>
<td>Full undos</td>
</tr>
<tr>
<td>partial undos</td>
<td>Partial undos</td>
</tr>
<tr>
<td>SACK undos</td>
<td>SACK undos</td>
</tr>
<tr>
<td>loss undos</td>
<td>Loss undos</td>
</tr>
<tr>
<td>segments lost</td>
<td>Segments lost</td>
</tr>
<tr>
<td>lost retransmits</td>
<td>Lost retransmits</td>
</tr>
<tr>
<td>TCP Reno failures</td>
<td>TCP Reno failures</td>
</tr>
<tr>
<td>SACK failures</td>
<td>SACK failures</td>
</tr>
<tr>
<td>loss failures</td>
<td>Loss failures</td>
</tr>
<tr>
<td>fast retransmits</td>
<td>Fast retransmits</td>
</tr>
<tr>
<td>forward retransmits</td>
<td>Forward retransmits</td>
</tr>
<tr>
<td>retransmits in slow start</td>
<td>Retransmits in slow start</td>
</tr>
</tbody>
</table>
### Table 16-5: Parameters in the output of the `show ip traffic` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeouts</td>
<td>Timeouts</td>
</tr>
<tr>
<td>TCP Reno recovery failures</td>
<td>TCP Reno recovery failures</td>
</tr>
<tr>
<td>SACK recovery failures</td>
<td>SACK recovery failures</td>
</tr>
<tr>
<td>collapsed segments received</td>
<td>Collapsed segments received</td>
</tr>
<tr>
<td>DSACKs sent for old packets</td>
<td>DSACKs sent for old packets</td>
</tr>
<tr>
<td>DSACKs sent for out of order segments</td>
<td>DSACKs sent for out of order segments</td>
</tr>
<tr>
<td>DSACKs received</td>
<td>DSACKs received</td>
</tr>
<tr>
<td>DSACKs received for out of order segments</td>
<td>DSACKs received for out of order segments</td>
</tr>
<tr>
<td>connections reset due to unexpected SYN</td>
<td>Connections reset due to unexpected SYN</td>
</tr>
<tr>
<td>connections reset due to unexpected data</td>
<td>Connections reset due to unexpected data</td>
</tr>
<tr>
<td>connections reset due to early user close</td>
<td>Connections reset due to early user close</td>
</tr>
<tr>
<td>connections aborted due to lack of memory</td>
<td>Connections aborted due to lack of memory</td>
</tr>
<tr>
<td>connections aborted due to timeout</td>
<td>Connections aborted due to timeout</td>
</tr>
<tr>
<td>connections aborted due to lingering</td>
<td>Connections aborted due to lingering</td>
</tr>
<tr>
<td>connection aborts due to connection failure</td>
<td>Connection aborts due to connection failure</td>
</tr>
<tr>
<td>TCP memory pressure events</td>
<td>TCP memory pressure events</td>
</tr>
<tr>
<td>SACKs discarded</td>
<td>SACKs discarded</td>
</tr>
<tr>
<td>Old DSACKs ignored</td>
<td>Old DSACKs ignored</td>
</tr>
<tr>
<td>DSACKs ignored without undo</td>
<td>DSACKs ignored without undo</td>
</tr>
<tr>
<td>Spurious RTOs</td>
<td>Spurious RTOs</td>
</tr>
<tr>
<td>TCP MD5 Not Found</td>
<td>TCP MD5 Not Found</td>
</tr>
<tr>
<td>TCP MD5 Unexpected</td>
<td>TCP MD5 Unexpected</td>
</tr>
<tr>
<td>TCP SACKs shifted</td>
<td>TCP SACKs shifted</td>
</tr>
<tr>
<td>TCP SACKs merged</td>
<td>TCP SACKs merged</td>
</tr>
<tr>
<td>TCP SACK shift fallback</td>
<td>TCP SACK shift fallback</td>
</tr>
<tr>
<td>UDP</td>
<td>UDP Counters</td>
</tr>
<tr>
<td>UDPLite</td>
<td>UDPLite Counters</td>
</tr>
</tbody>
</table>
Table 16-5: Parameters in the output of the `show ip traffic` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP6</td>
<td>UDPv6 Counters</td>
</tr>
<tr>
<td>UDPLite6</td>
<td>UDPLitev6 Counters</td>
</tr>
<tr>
<td>datagrams received</td>
<td>Datagrams received</td>
</tr>
<tr>
<td>datagrams received for unknown port</td>
<td>Datagrams received for unknown port</td>
</tr>
<tr>
<td>datagram receive errors</td>
<td>Datagram receive errors</td>
</tr>
<tr>
<td>datagrams transmitted</td>
<td>Datagrams transmitted</td>
</tr>
<tr>
<td>datagrams received</td>
<td>Datagrams received</td>
</tr>
<tr>
<td>datagrams received for unknown port</td>
<td>Datagrams received for unknown port</td>
</tr>
<tr>
<td>datagram receive errors</td>
<td>Datagram receive errors</td>
</tr>
<tr>
<td>datagrams transmitted</td>
<td>Datagrams transmitted</td>
</tr>
</tbody>
</table>
tcpdump

**Overview**
GW, Feb 2015 AR3040S and AR4050S don't support VRF Lite for 5.4.5 GA.

Use this command to start a tcpdump, which gives the same output as the Unix-like tcpdump command to display TCP/IP traffic. Press <ctrl> + c to stop a running tcpdump.

**Syntax**
tcpdump <line>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;line&gt;</td>
<td>Specify the dump options. For more information on the options for this placeholder see <a href="http://www.tcpdump.org/tcpdump_man.html">http://www.tcpdump.org/tcpdump_man.html</a></td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
To start a tcpdump running to capture IP packets, enter the command:

```
awplus# tcpdump ip
```

**Output**
Figure 16-16: 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>}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The destination IPv4 address. The IPv4 address uses the format A.B.C.D.</td>
</tr>
<tr>
<td>&lt;hostname&gt;</td>
<td>The destination hostname.</td>
</tr>
</tbody>
</table>

**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.
Introduction

Overview  This chapter provides an alphabetical reference of commands used to configure IPv6. For more information, see the IPv6 Feature Overview and Configuration Guide.
**IPv6 COMMANDS**

**Command List**

- “clear ipv6 neighbors” on page 698
- “ipv6 address” on page 699
- “ipv6 address autoconfig” on page 701
- “ipv6 enable” on page 703
- “ipv6 forwarding” on page 705
- “ipv6 nd managed-config-flag” on page 706
- “ipv6 nd minimum-ra-interval” on page 707
- “ipv6 nd other-config-flag” on page 708
- “ipv6 nd prefix” on page 709
- “ipv6 nd ra-interval” on page 711
- “ipv6 nd ra-lifetime” on page 712
- “ipv6 nd raguard” on page 713
- “ipv6 nd reachable-time” on page 715
- “ipv6 nd retransmission-time” on page 716
- “ipv6 nd suppress-ra” on page 717
- “ipv6 neighbor” on page 718
- “ipv6 opportunistic-nd” on page 719
- “ipv6 route” on page 720
- “ping ipv6” on page 721
- “show ipv6 forwarding” on page 722
- “show ipv6 interface brief” on page 723
- “show ipv6 neighbors” on page 724
- “show ipv6 route” on page 725
- “show ipv6 route summary” on page 727
- “traceroute ipv6” on page 728
clear ipv6 neighbors

**Overview**  Use this command to clear all dynamic IPv6 neighbor entries.

**Syntax**  clear ipv6 neighbors

**Mode**  Privileged Exec

**Example**  awplus# clear ipv6 neighbors
IPV6 ADDRESS

ipv6 address

**Overview**
Use this command to set the IPv6 address of a VLAN interface and enable IPv6.

Use the optional eui64 parameter to derive the interface identifier of the IPv6 address from the MAC address of the interface. Note that the MAC address of the default VLAN is applied if the interface does not have a MAC address of its own when specifying the eui64 parameter.

Use the no variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

**Syntax**

```
ipv6 address <ipv6-addr/prefix-length> [eui64]

no ipv6 address <ipv6-addr/prefix-length> [eui64]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv6-addr/prefix-length&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td>eui64</td>
<td>EUI-64 is a method of automatically deriving the lower 64 bits of an IPv6 address, based on the switch’s MAC address. See the Usage section for more information.</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
If the eui64 parameter is specified then the lower 64 bits of the IPv6 address are appended with the same address that would be acquired through stateless address autoconfiguration (SLAAC) if the device received an RA (Router Advertisement) specifying this prefix. See ipv6 address autoconfig for a detailed command description and examples to enable and disable SLAAC. For more information, see “IPv6 EUI-64 Addressing” in the IPv6 Feature Overview and Configuration Guide.

Note that link-local addresses are retained in the system until they are negated by using the no variant of the command that established them. See the ipv6 enable command for more information.

Also note that the link-local address is retained in the system if the global address is removed using another command, which was not used to establish the link-local address. For example, if a link local address is established with the ipv6 enable command then it will not be removed using a no ipv6 address command.
**Examples**

To assign the IPv6 address 2001:0db8::a2/64 to the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

To assign the **eui64** derived address in the prefix 2001:db8::/48 to VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-fr-subif)# ipv6 address 2001:0db8::/48 eui64
```

To remove the **eui64** derived address in the prefix 2001:db8::/48 from VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-fr-subif)# no ipv6 address 2001:0db8::/48 eui64
```

**Validation Commands**

- show running-config
- show ipv6 interface brief
- show ipv6 route

**Related Commands**

- ipv6 address autoconfig
**ipv6 address autoconfig**

**Overview**  
Use this command to enable IPv6 stateless address autoconfiguration (SLAAC) for an interface. This configures an IPv6 address on an interface derived from the MAC address on the interface.

Use the `no` variant of this command to disable IPv6 SLAAC on an interface. Note that if no global addresses are left after removing all IPv6 autoconfigured addresses then IPv6 is disabled.

**Syntax**  
ipv6 address autoconfig  
no ipv6 address autoconfig

**Mode**  
Interface Configuration for a VLAN interface.

**Usage**  
The `ipv6 address autoconfig` command enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6, but does not enable IPv6 forwarding. See `ipv6 forwarding` command for further description and examples.

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 link-local addresses are retained in the system until they are negated by using the `no` variant of the command that established them. See the `ipv6 enable` command for more information.

Also note that the link-local address is retained in the system if the global address is removed using another command that was not used to establish the link-local address. For example, if a link local address is established with the `ipv6 enable` command then it will not be removed using a `no ipv6 address` command.

**Examples**  
To enable SLAAC on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address autoconfig
```
To disable SLAAC on the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address autoconfig
```

**Validation Commands**
- show running-config
- show ipv6 interface brief
- show ipv6 route

**Related Commands**
- ipv6 address
- ipv6 enable
**ipv6 enable**

**Overview**  
Use this command to enable IPv6 on an interface without an IPv6 global address for the interface. This enables IPv6 with a IPv6 link-local address, not an IPv6 global address.

Use the no variant of this command to disable IPv6 on an interface without a global address. Note the no variant of this command does not operate on an interface with an IPv6 global address or an interface configured for IPv6 stateless address autoconfiguration (SLAAC).

**Syntax**  
ipv6 enable
no ipv6 enable

**Mode**  
Interface Configuration for a VLAN interface.

**Usage**  
The ipv6 enable command automatically configures an IPv6 link-local address on the interface and enables the interface for IPv6 processing.

A link-local address is an IP (Internet Protocol) address that is only used for communications in the local network, or for a point-to-point connection. Routing does not forward packets with link-local addresses. IPv6 requires that a link-local address is assigned to each interface that has the IPv6 protocol enabled, and when addresses are assigned to interfaces for routing IPv6 packets.

Note that link-local addresses are retained in the system until they are negated by using the no variant of the command that established them.

Also note that the link-local address is retained in the system if the global address is removed using another command that was not used to establish the link-local address. For example, if a link local address is established with the ipv6 enable command then it will not be removed using a no ipv6 address command.

**Examples**  
To enable IPv6 with only a link-local IPv6 address on the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
```

To disable IPv6 with only a link-local IPv6 address on the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 enable
```

**Validation Commands**

- show running-config
- show ipv6 interface brief
- show ipv6 route
Related Commands

ipv6 address
ipv6 address autoconfig
**ipv6 forwarding**

**Overview**  
Use this command to turn on IPv6 unicast routing for IPv6 packet forwarding. Execute this command globally on your device prior to issuing `ipv6 enable` on individual interfaces.

Use this `no` variant of this command to turn off IPv6 unicast routing for IPv6 packet forwarding. Note IPv6 unicast routing for IPv6 packet forwarding 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.

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.

**Syntax**

```
ipv6 forwarding
no ipv6 forwarding
```

**Mode**  
Global Configuration

**Default**  
IPv6 unicast forwarding is disabled by default.

**Usage**  
Enable IPv6 unicast forwarding globally for all interface 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 this command as shown below:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
```

To disable IPv6 unicast routing, use the `no` variant of this command as shown below:

```
awplus# configure terminal
awplus(config)# no ipv6 forwarding
```

**Related Commands**  
`ipv6 enable`  
`ipv6 multicast-routing`
**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, flag unset.

**Syntax**  
```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

**Default**  Unset

**Mode**  Interface Configuration for a VLAN interface.

**Usage**  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 the VLAN interface `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 a VLAN interface.

Use the **no** variant of this command in Interface Configuration mode to remove the minimum RA interval for a VLAN interface.

**Syntax**
```
ipv6 nd minimum-ra-interval <seconds>
no ipv6 nd minimum-ra-interval [<seconds>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;seconds&gt;</td>
<td>Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 3 to 1350 seconds.</td>
</tr>
</tbody>
</table>

**Default**
The RA interval for a VLAN interface is unset by default.

**Mode**
Interface Configuration for a VLAN 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 60
```

**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.

**NOTE:** 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.

**Usage**
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 `vlan4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
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`
**ip6 nd prefix**

**Overview**  Use this command in Interface Configuration mode for a VLAN interface 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 a VLAN interface in Interface Configuration mode.

**Syntax**  

```
ip6 nd prefix <ipv6-prefix/length>  
ip6 nd prefix <ipv6-prefix/length> [<valid-lifetime>]  
ip6 nd prefix <ipv6-prefix/length>  <valid-lifetime><preferred-lifetime>  [no-autoconfig]  
ip6 nd prefix <ipv6-prefix/length>  <valid-lifetime><preferred-lifetime>  off-link  [no-autoconfig]  
no ip6 nd prefix  [<ipv6-addr/prefix-length>|all]  
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv6-prefix/length&gt;</code></td>
<td>The prefix to be advertised by the router advertisement message.</td>
</tr>
<tr>
<td></td>
<td>The IPv6 address prefix uses the format X:X::/prefix-length.</td>
</tr>
<tr>
<td></td>
<td>The prefix-length is usually set between 0 and 64. The default is X:X::/64.</td>
</tr>
<tr>
<td><code>&lt;valid-lifetime&gt;</code></td>
<td>The the period during which the specified IPv6 address prefix is valid.</td>
</tr>
<tr>
<td></td>
<td>This can be set to a value between 0 and 4294967295 seconds. The default</td>
</tr>
<tr>
<td></td>
<td>is 2592000 (30 days). Note that this period should be set to a value greater</td>
</tr>
<tr>
<td></td>
<td>than that set for the prefix preferred-lifetime.</td>
</tr>
<tr>
<td><code>&lt;preferred-lifetime&gt;</code></td>
<td>Specifies the IPv6 prefix preferred lifetime. This is the period during</td>
</tr>
<tr>
<td></td>
<td>which the IPv6 address prefix is considered a current (undeprecated) value.</td>
</tr>
<tr>
<td></td>
<td>After this period, the command is still valid but should not be used in</td>
</tr>
<tr>
<td></td>
<td>new communications. Set to a value between 0 and 4294967295 seconds. The</td>
</tr>
<tr>
<td></td>
<td>default is 604800 seconds (7 days). Note that this period should be set to</td>
</tr>
<tr>
<td></td>
<td>a value less than that set for the prefix valid-lifetime.</td>
</tr>
<tr>
<td>off-link</td>
<td>Specify the IPv6 prefix off-link flag. The default is flag set.</td>
</tr>
<tr>
<td>no-autoconfig</td>
<td>Specify the IPv6 prefix no autoconfiguration flag. Setting this flag</td>
</tr>
<tr>
<td></td>
<td>indicates that the prefix is not to be used for autoconfiguration. The</td>
</tr>
<tr>
<td></td>
<td>default is flag set.</td>
</tr>
<tr>
<td>all</td>
<td>Specify all IPv6 prefixes associated with the VLAN interface.</td>
</tr>
</tbody>
</table>

**Default**  Valid-lifetime default is 2592000 seconds (30 days). Preferred-lifetime default is 604800 seconds (7 days).

**Mode**  Interface Configuration for a VLAN interface.
**Usage**

This command specifies the IPv6 prefix flags that are advertised by the router advertisement message.

**Examples**

The following example configures the device to issue router advertisements on the VLAN interface `vlan4`, and advertises the address prefix of `2001:0db8::/64`.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64
```

The following example configures the device to issue router advertisements on the VLAN interface `vlan4`, and advertises the address prefix of `2001:0db8::/64` with a valid lifetime of 10 days and a preferred lifetime of 5 days.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
```

The following example configures the device to issue router advertisements on the VLAN interface `vlan4`, and advertises 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.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 43200 no-autoconfig
```

The following example resets router advertisements on the VLAN interface `vlan4`, so the address prefix of `2001:0db8::/64` is not advertised from the device.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/64
```

The following example resets all router advertisements on the VLAN interface `vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan4
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;seconds&gt;</td>
<td>Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 4 to 1800 seconds.</td>
</tr>
</tbody>
</table>

**Default**  600 seconds.

**Mode**  Interface Configuration for a VLAN interface.

**Usage**  Advertisement flags will not be transmitted unless you have applied the `ipv6 nd suppress-ra` command as shown in the example below.

**Example**  To set the advertisements interval on the VLAN interface `vlan4` to be 60 seconds, use the following commands:
```
awplus# configure terminal
awplus(config)# interface vlan4
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**
```plaintext
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.

**Usage**
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 `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 `vlan4`, use the following commands:
```
awplus# configure terminal
awplus(config)# interface vlan4
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 enabled by default.

**Mode**
Interface Configuration for a device port interface.

**Usage**
Router Advertisements (RAs) are used by Routers to announce themselves on the link. Applying RA Guard to a device port disallows Router Advertisements and redirect messages. RA Guard blocks RAs from untrusted hosts. Blocking RAs stops untrusted hosts from flooding malicious RAs and stops any misconfigured hosts from disrupting traffic on the local network.

Enabling RA Guard on a port blocks RAs from a connected host and indicates the port and host are untrusted. Disabling RA Guard on a port allows RAs from a connected host and indicates the port and host are trusted. Ports and hosts are trusted by default to allow RAs.

**Example**
To enable RA Guard on device ports `port1.0.2-1.0.12`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-1.0.12
awplus(config-if)# ipv6 nd raguard
```

To verify RA Guard is enabled on device port interface `port1.0.2`, use the command:

```
awplus# show running-config interface port1.0.2
```

To disable RA Guard on device ports `port1.0.2-1.0.12`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.12
awplus(config-if)# no ipv6 nd raguard
```

When RA Guard is disabled on a device port it is not displayed in `show running-config` output.
**Output**  Example output from a `show running-config interface` port1.0.2 to verify RA Guard:

```
! interface port1.0.2
   switchport mode access
   ipv6 nd raguard
!
```

**Related Commands**  `show running-config interface`
ip v6 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 <millisseconds>
no ipv6 nd reachable-time

Parameter | Description
---|---
<millisseconds> | 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.

Usage
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 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 vlan4 to be 1800000 milliseconds, enter the following commands:

awplus# configure terminal
awplus(config)# interface vlan4
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 vlan4 to an unspecified reachable-time (0 milliseconds), enter the following commands:

awplus# configure terminal
awplus(config)# interface vlan4
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 [ <milliseconds> ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;milliseconds&gt;</td>
<td>Time period in milliseconds. Valid values are from 1000 to 3600000.</td>
</tr>
</tbody>
</table>

**Default**
1000 milliseconds (1 second)

**Mode**
Interface Configuration for a VLAN 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 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 `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.

**Example**  To enable the transmission of router advertisements from the VLAN interface vlan4 on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd suppress-ra
```

**Related Commands**  
ipv6 nd ra-interval
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>
```

**Mode**  Global Configuration

**Usage**  Use this command to clear a specific IPv6 neighbor entry. To clear all dynamic address entries, use the clear ipv6 neighbors command.

**Example**  To create a static neighbor entry for IPv6 address 2001:0db8::a2, on vlan 4, MAC address 0000.cd28.0880, on port1.0.6, use the command:
```
awplus# configure terminal
awplus(config)# ipv6 neighbor 2001:0db8::a2 vlan4 0000.cd28.0880 port1.0.6
```

**Related Commands**  clear ipv6 neighbors
ipv6 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**  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

**Validation Commands**  show running-config interface
**ipv6 route**

**Overview**
Use this command to establish the distance for static routes of a network prefix.

Use the no variant of this command to disable the distance for static routes of the network prefix.

**Syntax**
```
ipv6 route <dest-prefix> <dest-prefix/length> 
{<gateway-ip>|<gateway-name>} [<distvalue>]
```
```
no ipv6 route <dest-prefix> <dest-prefix/length> 
{<gateway-ip>|<gateway-name>} [<distvalue>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;dest-prefix/length&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;gateway-ip&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;distvalue&gt;</td>
<td>Specifies the administrative distance for the route. Valid values are from 1 to 255.</td>
</tr>
<tr>
<td>&lt;gateway-name&gt;</td>
<td>Specifies the name of the gateway (or next hop) interface.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Example**
```
awplus# configure terminal
awplus(config)# ipv6 route myintname 322001:0db8::1/128
```

**Validation Commands**
show running-config
show ipv6 route
IPv6 COMMANDS
PING IPV6

**ping ipv6**

**Overview**  
This command sends a query to another IPv6 host (send Echo Request messages).

**NOTE:** Use of the `interface` parameter keyword, plus an interface or an interface range, with this command is only valid when pinging an IPv6 link local address.

**Syntax**  
```
ping ipv6 {<host>|<ipv6-address>} [repeat {<1-2147483647}>|continuous] [size <10-1452>] [interface <interface-list>] [timeout <1-65535>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv6-addr&gt;</code></td>
<td>The destination IPv6 address. The IPv6 address uses the format X:X::X:X.</td>
</tr>
<tr>
<td><code>&lt;hostname&gt;</code></td>
<td>The destination hostname.</td>
</tr>
<tr>
<td><code>repeat</code></td>
<td>Specify the number of ping packets to send.</td>
</tr>
<tr>
<td><code>&lt;1-2147483647&gt;</code></td>
<td>Specify repeat count. The default is 5.</td>
</tr>
<tr>
<td><code>size &lt;10-1452&gt;</code></td>
<td>The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>The interface or range of configured IP interfaces to use as the source in the IP header of the ping packet.</td>
</tr>
<tr>
<td><code>timeout</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax** show ipv6 forwarding

**Mode** User Exec and Privileged Exec

**Example**

```
awplus# show ipv6 forwarding
```

**Output** Figure 17-1: Example output from the `show ipv6 forwarding` command

```
ipv6 forwarding is on
```
show ipv6 interface brief

**Overview** Use this command to display brief information about interfaces and the IPv6 address assigned to them.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**

```
show ipv6 interface [brief]
```

**Parameter** | Description
---|---
brief | Specify this optional parameter to display brief IPv6 interface information.

**Mode** User Exec and Privileged Exec

**Examples**

```
awplus# show ipv6 interface brief
```

**Output**

Figure 17-2: Example output from the `show ipv6 interface brief` command

<table>
<thead>
<tr>
<th>Interface</th>
<th>IPv6-Address</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>lo</td>
<td>unassigned</td>
<td>admin up</td>
<td>running</td>
</tr>
<tr>
<td>vlan1</td>
<td>2001:db8::1/48</td>
<td>admin up</td>
<td>down</td>
</tr>
<tr>
<td></td>
<td>fe80::215:77ff:fee9:5c50/64</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands**

`show interface brief`
show ipv6 neighbors

**Overview**  Use this command to display all IPv6 neighbors.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show ipv6 neighbors

**Mode**  User Exec and Privileged Exec
show ipv6 route

**Overview**
Use this command to display the IPv6 routing table for a protocol or from a particular table.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ipv6 route
[connected|database|ospf|rip|static|summary|<ipv6-address>|<ipv6-addr/prefix-length>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>Displays only the routes learned from connected interfaces.</td>
</tr>
<tr>
<td>database</td>
<td>Displays only the IPv6 routing information extracted from the database.</td>
</tr>
<tr>
<td>ospf</td>
<td>Displays only the routes learned from IPv6 Open Shortest Path First (OSPFv3).</td>
</tr>
<tr>
<td>rip</td>
<td>Displays only the routes learned from IPv6 Routing Information Protocol (RIPng).</td>
</tr>
<tr>
<td>static</td>
<td>Displays only the IPv6 static routes you have configured.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays summary information from the IPv6 routing table.</td>
</tr>
<tr>
<td>&lt;ipv6-address&gt;</td>
<td>Displays the routes for the specified address in the IP routing table. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.</td>
</tr>
<tr>
<td>&lt;ipv6-prefix/length&gt;</td>
<td>Displays only the routes for the specified IP prefix.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Example 1**
To display an IP route with all parameters turned on, use the following command:
```
awplus# show ipv6 route
```
### Output Figure 17-3: Example output of the `show ipv6 route` command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF   ::/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::14:0:0:0/64 via ::, vlan20
C  2001:db8::0:0:0:0/64 via ::, vlan30
C  2001:db8::28:0:0:0/64 via ::, vlan40
C  2001:db8::fa:0:0:0/64 via ::, vlan250
C  2001:db8::/64 via ::, vlan250
C  2001:db8::/64 via ::, vlan40
C  2001:db8::/64 via ::, vlan20
C  2001:db8::/64 via ::, vlan10
```

### Example 2
To display all database entries for an IP route, use the following command:
```
awplus# show ipv6 route database
```

### Output Figure 17-4: Example output of the `show ipv6 route database` command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF   > - selected route, * - FIB route, p - stale info
Timers: Uptime
S  ::/0 [1/0] via 2001::a:0:0:c0a8:a01 inactive, 6d22h12m
   [1/0] via 2001::fa:0:0:c0a8:fa01 inactive, 6d22h12m
```
**show ipv6 route summary**

**Overview**  
Use this command to display the summary of the current NSM RIB entries.  
For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
`show ipv6 route summary`

**Mode**  
User Exec and Privileged Exec

**Example**  
To display IP route summary, use the following command:

```
awplus# show ipv6 route summary
```

**Output**  
Figure 17-5: 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
ospf            5
Total            9
FIB              5
```
**tracert route ipv6**

- **Overview**: Use this command to trace the route to the specified IPv6 host.
- **Syntax**: `traceroute ipv6 {<ipv6-addr>|<hostname>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv6-addr&gt;</code></td>
<td>The destination IPv6 address. The IPv6 address uses the format X::X::X.</td>
</tr>
<tr>
<td><code>&lt;hostname&gt;</code></td>
<td>The destination hostname.</td>
</tr>
</tbody>
</table>

- **Mode**: User Exec and Privileged Exec
- **Example**: To run a tracert route for the IPv6 address 2001:0db8::a2, use the following command:
  
  ```bash
  awplus# traceroute ipv6 2001:0db8::a2
  ```

- **Related Commands**: ping ipv6
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 and the Routing Protocol Feature Overview and Configuration Guide.

Command List
• “ip route” on page 729
• “maximum-paths” on page 731
• “show ip route” on page 732
• “show ip route database” on page 735
• “show ip route summary” on page 737
**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>]  
```

**Mode**  Global Configuration

**Default**  The default administrative distance for a static route is 1 for priority over non-static routes.

**Usage**  Administrative distance can be modified so static routes do not 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`
ROUTING COMMANDS
MAXIMUM-PATHS

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-8&gt;</td>
<td>The maximum number of paths that a route can have in the FIB.</td>
</tr>
</tbody>
</table>

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  [connected|ospf|rip|static|<ip-addr>|<ip-addr/prefix-length>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>Displays only the routes learned from connected interfaces.</td>
</tr>
<tr>
<td>ospf</td>
<td>Displays only the routes learned from OSPF.</td>
</tr>
<tr>
<td>rip</td>
<td>Displays only the routes learned from RIP.</td>
</tr>
<tr>
<td>static</td>
<td>Displays only the static routes you have configured.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>Displays the routes for the specified address. Enter an IPv4 address.</td>
</tr>
<tr>
<td>&lt;ip-addr/prefix-length&gt;</td>
<td>Displays the routes for the specified network. Enter an IPv4 address and prefix length.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**  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 18-1: Example output from the `show ip route` command

<table>
<thead>
<tr>
<th>Codes:</th>
<th>C - connected, S - static, R - RIP</th>
<th>O - OSPF, IA - OSPF inter area</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>E1 - OSPF external type 1, E2 - OSPF external type 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* - candidate default</td>
<td></td>
</tr>
</tbody>
</table>

```
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       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**

```
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.

To avoid repetition, only selected route entries comprising of different elements are described here:

**OSPF Route**

```
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.
ROUTEING COMMANDS
SHOW IP ROUTE

**OSPF External Route**

```
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**

- `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`  
`[connected|ospf|rip|static]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>Displays only the routes learned from connected interfaces.</td>
</tr>
<tr>
<td>ospf</td>
<td>Displays only the routes learned from OSPF.</td>
</tr>
<tr>
<td>rip</td>
<td>Displays only the routes learned from RIP.</td>
</tr>
<tr>
<td>static</td>
<td>Displays only the static routes you have configured.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Example**  
To display the static routes in the RIB, use the command:

```
awplus# show ip route database static
```
ROUTING COMMANDS
SHOW IP ROUTE DATABASE

Output  Figure 18-2: Example output from the show ip route database command

Codes: C - connected, S - static, R - RIP, 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  * 17.17.17.32 [110/31] via 10.10.31.16, vlan2, 00:21:19
C  * 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

The routes added to the FIB are marked with a *. When multiple routes are available for the same prefix, the best route is indicated with the > symbol. All unselected routes have neither the * nor the > symbol.

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

These route entries denote:

- The same prefix was learned from OSPF and from static route configuration.
- Since this static route has a lower administrative distance than the OSPF route (110), the static route (1) is selected and installed in the FIB.

If the static route becomes unavailable, then the device automatically selects the OSPF route and installs it in the FIB.

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 18-3: Example output from the **show ip route summary** command

```
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source Networks
connected 5
ospf 2
Total 8
```
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.
RIP COMMANDS

Command List

• “accept-lifetime” on page 741
• “alliedware-behavior” on page 743
• “cisco-metric-behavior (RIP)” on page 745
• “clear ip rip route” on page 746
• “debug rip” on page 747
• “default-information originate (RIP)” on page 748
• “default-metric (RIP)” on page 749
• “distance (RIP)” on page 750
• “distribute-list (RIP)” on page 751
• “fullupdate (RIP)” on page 752
• “ip rip authentication key-chain” on page 753
• “ip rip authentication mode” on page 755
• “ip rip authentication string” on page 758
• “ip rip receive-packet” on page 760
• “ip rip receive version” on page 761
• “ip rip send-packet” on page 762
• “ip rip send version” on page 763
• “ip rip send version 1-compatible” on page 765
• “ip rip split-horizon” on page 767
• “key” on page 768
• “key chain” on page 769
• “key-string” on page 770
• “maximum-prefix” on page 771
• “neighbor (RIP)” on page 772
• “network (RIP)” on page 773
• “offset-list (RIP)” on page 774
• “passive-interface (RIP)” on page 775
• “recv-buffer-size (RIP)” on page 776
• “redistribute (RIP)” on page 777
• “restart rip graceful” on page 778
• “rip restart grace-period” on page 779
• “route (RIP)” on page 780
• “router rip” on page 781
• “send-lifetime” on page 782
• “show debugging rip” on page 784
RIP COMMANDS

- “show ip protocols rip” on page 785
- “show ip rip” on page 786
- “show ip rip database” on page 787
- “show ip rip interface” on page 788
- “timers (RIP)” on page 789
- “undebug rip” on page 791
- “version” on page 792
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;start-date&gt;</code></td>
<td>Specifies the start period - time and date in the format DD MMM YYYY or MMM DD YYYY:<a href="">hh:mm:ss</a>{&lt;day&gt; &lt;month&gt; &lt;year&gt;</td>
</tr>
<tr>
<td><code>&lt;hh:mm:ss&gt;</code></td>
<td>Time of the day when accept-lifetime starts, in hours, minutes and seconds</td>
</tr>
<tr>
<td><code>&lt;day&gt;</code></td>
<td><code>&lt;1-31&gt;</code> Specifies the day of the month to start.</td>
</tr>
<tr>
<td><code>&lt;month&gt;</code></td>
<td>Specifies the month of the year to start (the first three letters of the month, for example, Jan).</td>
</tr>
<tr>
<td><code>&lt;year&gt;</code></td>
<td><code>&lt;1993-2035&gt;</code> Specifies the year to start.</td>
</tr>
<tr>
<td><code>&lt;end-date&gt;</code></td>
<td>Specifies the end period - time and date in the format DD MMM YYYY or MMM DD YYYY:<a href="">hh:mm:ss</a>{&lt;day&gt; &lt;month&gt; &lt;year&gt;</td>
</tr>
<tr>
<td><code>&lt;hh:mm:ss&gt;</code></td>
<td>Time of the day when lifetime expires, in hours, minutes and seconds.</td>
</tr>
<tr>
<td><code>&lt;day&gt;</code></td>
<td><code>&lt;1-31&gt;</code> Specifies the day of the month to expire.</td>
</tr>
<tr>
<td><code>&lt;month&gt;</code></td>
<td>Specifies the month of the year to expire (the first three letters of the month, for example, Feb).</td>
</tr>
<tr>
<td><code>&lt;year&gt;</code></td>
<td><code>&lt;1993-2035&gt;</code> Specifies the year to expire.</td>
</tr>
<tr>
<td><code>&lt;seconds&gt;</code></td>
<td><code>&lt;1-2147483646&gt;</code> Duration of the key in seconds.</td>
</tr>
<tr>
<td><code>infinite</code></td>
<td>Never expires.</td>
</tr>
</tbody>
</table>

**Mode**

Keychain-key Configuration
**RIP Commands**

**ACCEPT-LIFETIME**

**Examples**

The following examples show the setting of accept-lifetime for key1 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 Dec 3 2007 04:04:02 Oct 6 2008
```

or:

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# accept-lifetime 03:03:01 3 Dec 2007 04:04:02 6 Oct 2008
```

**Related Commands**

- `key`
- `key-string`
- `key chain`
- `send-lifetime`
**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}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rip1-send</td>
<td>Configures the router to behave in AlliedWare mode when <strong>sending</strong> update messages.</td>
</tr>
<tr>
<td>rip1-recv</td>
<td>Configures the router to behave in AlliedWare mode when <strong>receiving</strong> update messages.</td>
</tr>
</tbody>
</table>

**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, the prefix 192.168.1.144 would be sent as-is.

**Mode**

Router Configuration

**Examples**

To configure your device for **alliedware-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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables updating the metric consistent with Cisco.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables updating the metric consistent with Cisco.</td>
</tr>
</tbody>
</table>

**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`
RIP Commands

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>|static|connected|rip|ospf|all}
```

Mode
Privileged Exec

Usage
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>RIP events debug information is displayed.</td>
</tr>
<tr>
<td>nsm</td>
<td>RIP and NSM communication is displayed.</td>
</tr>
<tr>
<td>&lt;packet&gt;</td>
<td>packet [recv</td>
</tr>
<tr>
<td>recv</td>
<td>Specifies that information for received packets be displayed.</td>
</tr>
<tr>
<td>send</td>
<td>Specifies that information for sent packets be displayed.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays detailed information for the sent or received packet.</td>
</tr>
<tr>
<td>all</td>
<td>Displays all RIP debug information.</td>
</tr>
</tbody>
</table>

**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>]

**Default**  
By default, the RIP metric value is set to 1.

**Mode**  
RIP Router Configuration

**Usage**  
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). See 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-255&gt;</td>
<td>The administrative distance value you are setting for this RIP route.</td>
</tr>
<tr>
<td>&lt;ip-addr/prefix-length&gt;</td>
<td>The network IP address and prefix-length that you are changing the administrative distance for.</td>
</tr>
<tr>
<td>&lt;access-list&gt;</td>
<td>Specifies the access-list name. This access list specifies which routes within the network &lt;ip-address/m&gt; this command applies to.</td>
</tr>
</tbody>
</table>

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
RIP COMMANDS
DISTRIBUTE-LIST (RIP)

**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>]
```

**Default**
Disabled

**Mode**
RIP Router Configuration

**Usage**
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 allow 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**  Use the following commands to enable the fullupdate (RIP) function:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# fullupdate
```
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;key-chain-name&gt;</td>
<td>Specify the name of the key chain. This is an alpha-numeric string, but it cannot include spaces.</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
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 sample multiple keys authentication RIP configuration, 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 Apr 08 2008 duration 43200
awplus(config-keychain-key)# send-lifetime 10:00:00 Apr 08 2008 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
awplus(config-if)# exit
awplus(config)# exit
awplus#
```

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>md5</td>
<td>Uses the keyed MD5 authentication algorithm.</td>
</tr>
<tr>
<td>text</td>
<td>Specifies clear text or simple password authentication.</td>
</tr>
</tbody>
</table>

**Default**
Text authentication is enabled

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
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}
   ```
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 sample multiple keys authentication RIP configuration, 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 Apr 08 2008 duration 43200
awplus(config-keychain-key)# send-lifetime 10:00:00 Apr 08 2008 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
awplus(config-if)# exit
awplus(config)# exit
awplus#
```
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;auth-string&gt;</td>
<td>The authentication string or password used by a key. It is an alphanumeric string and can include spaces.</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
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
```
RIP COMMANDS

IP RIP AUTHENTICATION STRING

**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` command.

**Syntax**
```
ip rip receive version {1|2}
no ip rip receive version
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Specifies acceptance of RIP version 1 packets on the interface.</td>
</tr>
<tr>
<td>2</td>
<td>Specifies acceptance of RIP version 2 packets on the interface.</td>
</tr>
</tbody>
</table>

**Default**
Version 2

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
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` 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`
**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`:

```bash
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` 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` 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**

This command applies to a specific interface and overrides the version specified by the `version` 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` 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`
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 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-compatible</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Default**  RIP version 2 is enabled by default.

**Mode**  Interface Configuration for a VLAN interface.

**Usage**  This command applies to a specific interface and overrides the version specified by the version 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 command.

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# no ip rip send version
```
RIP COMMANDS
IP RIP SEND VERSION 1-COMPATIBLE

Related Commands
ip rip send version
version
**ip rip split-horizon**

**Overview**  
Use this command to perform the split-horizon action on the interface. The default is split-horizon poisoned.

Use the **no** variant of this command to disable this function.

**Syntax**  
```
ip rip split-horizon [poisoned]
no ip rip split-horizon
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>poisoned</td>
<td>Performs split-horizon with poisoned reverse.</td>
</tr>
</tbody>
</table>

**Default**  
Split horizon poisoned is the default.

**Mode**  
Interface Configuration for a VLAN interface.

**Usage**  
This command can only be used on VLAN interfaces.

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.

**Example**  
To perform the split-horizon action on, use the following command:

```
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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;keyid&gt;</td>
<td>&lt;0-2147483647&gt; Key identifier number.</td>
</tr>
</tbody>
</table>

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**  
```plaintext
key chain <key-chain-name>
no key chain <key-chain-name>
```

**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.

```plaintext
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)#
```

**Related Commands**
- `key`
- `key-string`
- `accept-lifetime`
- `send-lifetime`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;key-chain-name&gt;</code></td>
<td>Specify the name of the key chain to manage.</td>
</tr>
</tbody>
</table>
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
```

**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
```

**Parameter** | **Description**
---|---
`<key-password>` | A string of characters to be used as a password by the key.

**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
```

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;maxprefix&gt;</code></td>
<td><code>&lt;1-65535&gt;</code> The maximum number of RIP routes allowed.</td>
</tr>
<tr>
<td><code>&lt;threshold&gt;</code></td>
<td><code>&lt;1-100&gt;</code> Percentage of maximum routes to generate a warning. The default threshold is 75%.</td>
</tr>
</tbody>
</table>
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-prefix-length>]|<vlan-name>}
network {<network-address>[/<subnet-mask>]|<vlan-name>}
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;network-address&gt;[/&lt;subnet-prefix-length&gt;]</code></td>
<td>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, i.e. an IP address of 10.0.0.0 will have a prefix length of 8 applied to it.</td>
</tr>
<tr>
<td><code>&lt;vlan-name&gt;</code></td>
<td>Specify a VLAN name with up to 32 alphanumeric characters to run RIP.</td>
</tr>
</tbody>
</table>

**Default**
Disabled

**Mode**
RIP Router Configuration

**Usage**
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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;access-list&gt;</td>
<td>Specifies the access-list number or names to apply.</td>
</tr>
<tr>
<td>in</td>
<td>Indicates the access list will be used for metrics of incoming advertised routes.</td>
</tr>
<tr>
<td>out</td>
<td>Indicates the access list will be used for metrics of outgoing advertised routes.</td>
</tr>
<tr>
<td>&lt;offset&gt;</td>
<td>&lt;0-16&gt; Specifies that the offset is used for metrics of networks matching the access list.</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>An alphanumeric string that specifies the interface to match.</td>
</tr>
</tbody>
</table>

**Default**
The default offset value is the metric value of the interface over which the updates are being exchanged.

**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.

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# offset-list 8 in 5 vlan2
```
RIP COMMANDS
PASSIVE-INTERFACE (RIP)

**passive-interface (RIP)**

**Overview**  Use this command to block RIP broadcasts on the VLAN interface. Use the no variant of this command to disable this function.

**Syntax**  
```
passive-interface <interface>
no passive-interface <interface>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>Specifies the interface name.</td>
</tr>
</tbody>
</table>

**Default**  Disabled

**Mode**  RIP Router Configuration

**Usage**  This command can only be configured for VLAN interfaces.

**Examples**  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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;8192-2147483647&gt;</td>
<td>Specify the RIP UDP (User Datagram Protocol) buffer size value in bits.</td>
</tr>
</tbody>
</table>

**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 on this command, but have no effect.

**Syntax**
```
redistribute {connected|static|ospf} [metric <0-16>] [routemap <routemap>]
no redistribute {connected|static|ospf} [metric] [routemap]
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routemap</td>
<td>Optional. Specifies route-map that controls how routes are redistributed.</td>
</tr>
<tr>
<td>&lt;routemap&gt;</td>
<td>Optional. The name of the route map.</td>
</tr>
<tr>
<td>connected</td>
<td>Redistribute from connected routes.</td>
</tr>
<tr>
<td>static</td>
<td>Redistribute from static routes.</td>
</tr>
<tr>
<td>ospf</td>
<td>Redistribute from Open Shortest Path First (OSPF).</td>
</tr>
<tr>
<td>metric &lt;0-16&gt;</td>
<td>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 <code>default-metric (RIP)</code> command, the default is one.</td>
</tr>
</tbody>
</table>

**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**  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`.

When a master failover happens on a VCStack, the RIP grace-period will apply the larger value of either, the setting's configured value, or its default of 60 seconds.

**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 Commands
RIP Restart Grace-Period

**ripl 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>
norip restart grace-period <1-65535>

**Mode**
Global Configuration

**Default**
The default RIP grace-period is 60 seconds.

**Usage**
Use this command to enable the **Graceful Restart** feature on the RIP process.
Entering this command configures a grace period for RIP.

When a master failover happens on a VCStack, the RIP grace-period will be the longest period between the default value (60 seconds is the default RIP grace-period) and the configured RIP grace-period value from this command. So the configured RIP grace-period value will not be used for a VCStack master failover if it is shorter than the default RIP grace-period value.

**Example**
awplus# configure terminal
awplus(config)# rip restart grace-period 200
**route (RIP)**

**Overview**
Use this command to configure static RIP routes. Use the `no` variant of this command to disable this function.

**Syntax**
```
route <ip-addr/prefix-length>
no route <ip-addr/prefix-length>
```

**Default**
No static RIP route is added by default.

**Mode**
RIP Router Configuration

**Usage**
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`
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| <start-date> | Specifies the start period - time and date in the format DD MMM YYYY or MMM DD YYYY: 
|             | `<hh:mm:ss>{<day> <month> <year> | <month> <day> <year>}` |
|             | `<hh:mm:ss>` Time of the day when send-lifetime starts, in hours, minutes and seconds |
|             | `<day>` <1-31> Specifies the day of the month to start.                      |
|             | `<month>` Specifies the month of the year to start (the first three letters of the month, for example, Jan). |
|             | `<year>` <1993-2035> Specifies the year to start.                           |
| <end-date>  | Specifies the end period - time and date in the format DD MMM YYYY or MMM DD YYYY: 
|             | `<hh:mm:ss>{<day> <month> <year> | <month> <day> <year>}` |
|             | `<hh:mm:ss>` Time of the day when lifetime expires, in hours, minutes and seconds. |
|             | `<day>` <1-31> Specifies the day of the month to expire.                    |
|             | `<month>` Specifies the month of the year to expire (the first three letters of the month, for example, Feb). |
|             | `<year>` <1993-2035> Specifies the year to expire.                         |
| <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 key1 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 2004 04:04:02 Dec 6 2006
```
RIP COMMANDS

SEND-LIFETIME

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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show debugging rip

**Mode**  User Exec and Privileged Exec

**Usage**  Use this command to display the debug status of RIP.

**Example**  awplus# show debugging rip
show ip protocols rip

**Overview**  
Use this command to display RIP process parameters and statistics.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show ip protocols rip

**Mode**  
User Exec and Privileged Exec

**Example**  
awplus# show ip protocols rip

**Output**  
Figure 19-1: 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 “Controlling “show” Command Output” in 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 19-2: Example output from the `show up rip` command

```
awplus# show ip rip
Codes: R - RIP, Rc - RIP connected, Rs - RIP static
       C - Connected, S - Static, O - OSPFNetwork
Metric From If    Time   Next Hop
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 “Controlling “show” Command Output” in 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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>The interface to display information about. For instance: vlan2.</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;update&gt;</code></td>
<td><code>&lt;5-2147483647&gt;</code>&lt;br&gt;Specifies the period at which RIP route update packets are transmitted. The default is 30 seconds.</td>
</tr>
<tr>
<td><code>&lt;timeout&gt;</code></td>
<td><code>&lt;5-2147483647&gt;</code>&lt;br&gt;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.</td>
</tr>
<tr>
<td><code>&lt;garbage&gt;</code></td>
<td><code>&lt;5-2147483647&gt;</code>&lt;br&gt;Specifies the routing garbage collection timer in seconds. The default is 120 seconds.</td>
</tr>
</tbody>
</table>

**Default**
Enabled

**Mode**
RIP Router Configuration

**Usage**
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 adjust router network timers to 30 180 120, use the following command:
```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# timers basic 30 180 120
```
To adjust router network timers to 30 180 120 with VRF, use the following command:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# address-family ipv4 vrf blue
awplus(config-router-af)# 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>}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Disables all RIP debugging.</td>
</tr>
<tr>
<td>events</td>
<td>Disables the logging of RIP events.</td>
</tr>
<tr>
<td>nsm</td>
<td>Disables the logging of RIP and NSM communication.</td>
</tr>
<tr>
<td>&lt;packet&gt;</td>
<td>packet [recv</td>
</tr>
<tr>
<td>recv</td>
<td>Disables the logging of received packet information.</td>
</tr>
<tr>
<td>send</td>
<td>Disables the logging of sent packet information.</td>
</tr>
<tr>
<td>detail</td>
<td>Disables the logging of sent or received RIP packets.</td>
</tr>
</tbody>
</table>

**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

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

**Default**  Version 2

**Mode**  RIP Router Configuration

**Usage**  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` 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
```

**Validation Commands**  
```
awplus#show running-config

! router rip
  version 1
!
```

**Related Commands**  `ip rip receive version`, `ip rip send version`
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 793
- “clear ipv6 rip route” on page 794
- “debug ipv6 rip” on page 795
- “default-information originate (IPv6 RIPng)” on page 796
- “default-metric (IPv6 RIPng)” on page 797
- “distribute-list (IPv6 RIPng)” on page 798
- “ipv6 rip metric-offset” on page 799
- “ipv6 rip split-horizon” on page 801
- “ipv6 router rip” on page 802
- “neighbor (IPv6 RIPng)” on page 803
- “offset-list (IPv6 RIPng)” on page 804
- “passive-interface (IPv6 RIPng)” on page 805
- “recv-buffer-size (IPv6 RIPng)” on page 806
- “redistribute (IPv6 RIPng)” on page 807
- “route (IPv6 RIPng)” on page 808
- “router ipv6 rip” on page 809
- “show debugging ipv6 rip” on page 810
- “show ipv6 protocols rip” on page 811
- “show ipv6 rip” on page 812
- “show ipv6 rip database” on page 813
- “show ipv6 rip interface” on page 814
- “timers (IPv6 RIPng)” on page 815
- “undebug ipv6 rip” on page 816
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**

```plaintext
aggregate-address <ipv6-addr/prefix-length>
no aggregate-address <ipv6-addr/prefix-length>
```

**Parameter**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the IPv6 Address in the format X:X::X:X/Prefix-Length. The prefix-length is a decimal integer between 1 and 128.</td>
</tr>
</tbody>
</table>

**Mode**

Router Configuration

**Usage**

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**

```plaintext
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv6-addr/prefix-length&gt;</code></td>
<td>Specify the IPv6 Address in format <code>X:X:XX/Prefix-Length</code>. The prefix-length is a decimal integer between 1 and 128. Removes entries which exactly match this destination address from the RIPng routing table.</td>
</tr>
<tr>
<td><code>connected</code></td>
<td>Removes redistributed connected entries from RIPng routing table.</td>
</tr>
<tr>
<td><code>static</code></td>
<td>Removes redistributed static entries from the RIPng routing table.</td>
</tr>
<tr>
<td><code>rip</code></td>
<td>Removes RIPng routes from the RIPng routing table.</td>
</tr>
<tr>
<td><code>ospf</code></td>
<td>Removes redistributed OSPFv3 routes from the RIPng routing table.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Clears the entire RIPng routing table.</td>
</tr>
</tbody>
</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**  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all RIPng debugging showing RIPng events debug information, RIPng received packets information, and RIPng sent packets information.</td>
</tr>
<tr>
<td>events</td>
<td>Displays RIPng events debug information.</td>
</tr>
<tr>
<td>nsm</td>
<td>Displays RIPng and NSM communication.</td>
</tr>
<tr>
<td>packet</td>
<td>Displays RIPng packets only.</td>
</tr>
<tr>
<td>recv</td>
<td>Displays information for received packets.</td>
</tr>
<tr>
<td>send</td>
<td>Displays information for sent packets.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays detailed information for the sent or received packet.</td>
</tr>
</tbody>
</table>

**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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-16&gt;</td>
<td>Metric value.</td>
</tr>
</tbody>
</table>

**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)`
**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]
```

**Parameter**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;access-list&gt;</td>
</tr>
<tr>
<td>Specifies the IPv6 access-list number or name to use.</td>
</tr>
<tr>
<td>&lt;prefix-list-name&gt;</td>
</tr>
<tr>
<td>Filter prefixes in routing updates. Specify the name of the IPv6 prefix-list to use.</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
</tr>
<tr>
<td>The interface for which distribute-list applies. For instance: vlan2.</td>
</tr>
<tr>
<td>in</td>
</tr>
<tr>
<td>Filter incoming routing updates.</td>
</tr>
<tr>
<td>out</td>
</tr>
<tr>
<td>Filter outgoing routing updates.</td>
</tr>
</tbody>
</table>

**Default**

Disabled

**Mode**

Router Configuration

**Usage**

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
RIPng for IPv6 Commands
IPv6 RIP Metric-Offset

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>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-16&gt;</td>
<td>Specify an increment to the metric value on an incoming route. The metric value for RIPng routes is the hop count for the route.</td>
</tr>
</tbody>
</table>

Default
The default RIPng metric value is 1.

Usage
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.

**Usage** 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.

**Usage**
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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv6-link-local-addr&gt;</code></td>
<td>Specify the link-local IPv6 address (in the format <code>X:X::X:X</code>) of a neighboring router to exchange routing information with.</td>
</tr>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>The interface. For instance: <code>vlan2</code>.</td>
</tr>
</tbody>
</table>

**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>]
```

**Default**
The default offset value is the metric value of the interface over which the updates are being exchanged.

**Mode**
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.

**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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>The interface. For instance: vlan2.</td>
</tr>
</tbody>
</table>

**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**

```plaintext
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 UDP, use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# recv-buffer-size 23456789
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# no recv-buffer-size 23456789
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# no recv-buffer-size
```
redistribute (IPv6 RIPng)

**Overview**
Use this command to redistribute information from other routing protocols into RIPng.

Use the `no` variant of this command to disable the specified redistribution. The parameters `metric` and `route-map` may be used on this command, but have no effect.

**Syntax**
```
redistribute {connected|static|ospf} [metric <0-16>] [route-map <route-map>]
no redistribute {connected|static|ospf} [metric <0-16>] [route-map <route-map>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;0-16&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;route-map&gt;</code></td>
<td>Optional. Specifies route-map to be used to redistribute information.</td>
</tr>
<tr>
<td><code>connected</code></td>
<td>Redistribute from connected routes.</td>
</tr>
<tr>
<td><code>static</code></td>
<td>Redistribute from static routes.</td>
</tr>
<tr>
<td><code>ospf</code></td>
<td>Redistribute from Open Shortest Path First (OSPF).</td>
</tr>
</tbody>
</table>

**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**

```plaintext
route <ipv6-addr/prefix-length>
no route <ipv6-addr/prefix-length>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv6-addr/prefix-length&gt;</code></td>
<td>Specify the IPv6 Address in format <code>X:XX:XX/Prefix-Length</code>. The prefix-length is a decimal integer between 1 and 128.</td>
</tr>
</tbody>
</table>

**Mode**
Router Configuration

**Usage**
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:

```plaintext
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 display the RIPng debugging status for the debugging options of: nsm debugging, RIPng event debugging, RIPng packet debugging, and RIPng nsm debugging.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show debugging ipv6 rip

**Mode**  User Exec and Privileged Exec

**Usage**  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 protocols rip

**Overview**  Use this command to display RIPng process parameters and statistics.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show ipv6 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
  Redistribution:
  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 “Controlling “show” Command Output” in 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:

```bash
awplus# show ipv6 rip
```

**Output**

```
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show ipv6 rip database [full]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>full</td>
<td>Display all IPv6 RIPng full database entries including sub-optimal routes.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Example**  
To display information about the RIPng database, use the following command:

```
awplus# show ipv6 rip database
```

**Output**

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>If</th>
<th>Met</th>
<th>Tag</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>R 2001:db8:1::/48</td>
<td>2001:db8:2::/48</td>
<td>vlan3</td>
<td>3</td>
<td>0</td>
<td>02:28</td>
</tr>
<tr>
<td>C 2001:db8:3::/48</td>
<td>::</td>
<td>vlan2</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Ra 2001:db8:4::/48</td>
<td>--</td>
<td></td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Rs 2001:db8:5::/48</td>
<td>2001:db8:1::/48</td>
<td>vlan3</td>
<td>3</td>
<td>0</td>
<td>02:32</td>
</tr>
<tr>
<td>Cs 2001:db8:6::/48</td>
<td>::</td>
<td>vlan3</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  `show ipv6 rip interface [interface]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>The interface to display information about. For instance: <code>vlan2</code>.</td>
</tr>
</tbody>
</table>

**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
```
RIPng for IPv6 Commands
Timers (IPv6 RIPng)

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;update&gt;</td>
<td>&lt;5-2147483647&gt; Specifies the RIPng routing table update timer in seconds. The default is 30 seconds.</td>
</tr>
<tr>
<td>&lt;timeout&gt;</td>
<td>&lt;5-2147483647&gt; 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.</td>
</tr>
<tr>
<td>&lt;garbage&gt;</td>
<td>&lt;5-2147483647&gt; Specifies the RIPng routing garbage collection timer in seconds. The default is 120 seconds.</td>
</tr>
</tbody>
</table>

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]]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Disables all RIPng debugging.</td>
</tr>
<tr>
<td>events</td>
<td>Disable the display of RIPng events information.</td>
</tr>
<tr>
<td>nsm</td>
<td>Disable the display of RIPng and NSM communication.</td>
</tr>
<tr>
<td>packet</td>
<td>Disable debugging of specified RIPng packets only.</td>
</tr>
<tr>
<td>recv</td>
<td>Disable the display of information for received packets.</td>
</tr>
<tr>
<td>send</td>
<td>Disable the display of information for sent packets.</td>
</tr>
<tr>
<td>detail</td>
<td>Disable the display of detailed information for sent or received packets.</td>
</tr>
</tbody>
</table>

**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`
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.
OSPF COMMANDS

Command List

- “area default-cost” on page 820
- “area authentication” on page 821
- “area filter-list” on page 822
- “area nssa” on page 823
- “area range” on page 825
- “area stub” on page 827
- “area virtual-link” on page 828
- “auto-cost reference bandwidth” on page 831
- “bandwidth” on page 833
- “capability opaque” on page 834
- “capability restart” on page 835
- “clear ip ospf process” on page 836
- “compatible rfc1583” on page 837
- “debug ospf events” on page 838
- “debug ospf ifsm” on page 839
- “debug ospf ls” on page 840
- “debug ospf nsm” on page 841
- “debug ospf nsm” on page 842
- “debug ospf packet” on page 843
- “debug ospf route” on page 844
- “default-information originate (OSPF)” on page 845
- “default-metric (OSPF)” on page 846
- “distance (OSPF)” on page 847
- “distribute-list (OSPF)” on page 849
- “enable db-summary-opt” on page 851
- “host area” on page 852
- “ip ospf authentication” on page 853
- “ip ospf authentication-key” on page 854
- “ip ospf cost” on page 855
- “ip ospf database-filter” on page 856
- “ip ospf dead-interval” on page 857
- “ip ospf disable all” on page 858
- “ip ospf hello-interval” on page 859
- “ip ospf message-digest-key” on page 860
- “ip ospf mtu” on page 862
OSPF COMMANDS

- “ip ospf mtu-ignore” on page 863
- “ip ospf network” on page 864
- “ip ospf priority” on page 865
- “ip ospf resync-timeout” on page 866
- “ip ospf retransmit-interval” on page 867
- “ip ospf transmit-delay” on page 868
- “max-concurrent-dd” on page 869
- “maximum-area” on page 870
- “neighbor (OSPF)” on page 871
- “network area” on page 872
- “ospf abr-type” on page 873
- “ospf restart grace-period” on page 874
- “ospf restart helper” on page 875
- “ospf router-id” on page 877
- “overflow database” on page 878
- “overflow database external” on page 879
- “passive-interface (OSPF)” on page 880
- “redistribute (OSPF)” on page 881
- “restart ospf graceful” on page 883
- “router ospf” on page 884
- “router-id” on page 885
- “show debugging ospf” on page 886
- “show ip ospf” on page 887
- “show ip ospf border-routers” on page 890
- “show ip ospf database” on page 891
- “show ip ospf database asbr-summary” on page 893
- “show ip ospf database external” on page 894
- “show ip ospf database network” on page 896
- “show ip ospf database nssa-external” on page 898
- “show ip ospf database opaque-area” on page 900
- “show ip ospf database opaque-as” on page 901
- “show ip ospf database opaque-link” on page 902
- “show ip ospf database router” on page 903
- “show ip ospf database summary” on page 905
- “show ip ospf interface” on page 908
OSPF COMMANDS

- “show ip ospf neighbor” on page 909
- “show ip ospf route” on page 911
- “show ip ospf virtual-links” on page 912
- “show ip protocols ospf” on page 913
- “summary-address” on page 914
- “timers spf exp” on page 915
- “undebug ospf events” on page 916
- “undebug ospf ifsm” on page 917
- “undebug ospf lsa” on page 918
- “undebug ospf nfsm” on page 919
- “undebug ospf nsm” on page 920
- “undebug ospf packet” on page 921
- “undebug ospf route” on page 922
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
```

**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**
```plaintext
area <area-id> authentication [message-digest]
noc area <area-id> authentication
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>The OSPF area that you are enabling authentication for. This can be entered in either dotted decimal format.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>OSPF Area ID expressed in IPv4 address, entered in the form A.B.C.D.</td>
</tr>
<tr>
<td>&lt;0-4294967295&gt;</td>
<td>OSPF Area ID expressed as a decimal number within the range shown.</td>
</tr>
<tr>
<td>message-digest</td>
<td>Enables MD5 authentication in the OSPF area.</td>
</tr>
</tbody>
</table>

**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**
```plaintext
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>|prefix <prefix-list>} {in|out}
no area <area-id> filter-list {access <access-list>|prefix <prefix-list>} {in|out}
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>OSPF Area ID expressed in IPv4 address format A.B.C.D.</td>
</tr>
<tr>
<td>&lt;0-4294967295&gt;</td>
<td>OSPF Area ID expressed as a decimal number within the range shown.</td>
</tr>
<tr>
<td>access</td>
<td>Use access-list to filter summary.</td>
</tr>
<tr>
<td>prefix</td>
<td>Use prefix-list to filter summary.</td>
</tr>
<tr>
<td>&lt;access-list&gt;</td>
<td>Name of an access-list.</td>
</tr>
<tr>
<td>&lt;prefix-list&gt;</td>
<td>Name of a prefix-list.</td>
</tr>
<tr>
<td>in</td>
<td>Filter routes from the other areas to this area.</td>
</tr>
<tr>
<td>out</td>
<td>Filter routes from this area to the other areas.</td>
</tr>
</tbody>
</table>

**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 ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>OSPF Area ID expressed in IPv4 address format A.B.C.D.</td>
</tr>
<tr>
<td>&lt;0-4294967295&gt;</td>
<td>OSPF Area ID expressed as a decimal number within the range shown.</td>
</tr>
<tr>
<td></td>
<td>For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.</td>
</tr>
<tr>
<td>default-information-originate</td>
<td>Originate Type-7 default LSA into NSSA.</td>
</tr>
<tr>
<td>&lt;metric&gt;</td>
<td>The external or internal metric. Specify the following:</td>
</tr>
<tr>
<td>metric&lt;0-16777214&gt;</td>
<td>The metric value.</td>
</tr>
<tr>
<td>metric-type&lt;1-2&gt;</td>
<td>External metric type.</td>
</tr>
<tr>
<td>no-redistribution</td>
<td>Do not redistribute external route into NSSA.</td>
</tr>
<tr>
<td>no-summary</td>
<td>Do not inject inter-area route into NSSA.</td>
</tr>
<tr>
<td>translator-role</td>
<td>Specify NSSA-ABR translator-role.</td>
</tr>
</tbody>
</table>


### OSPF Commands

#### AREA NSSA

**Mode**
Router Configuration

**Example**

```bash
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

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;role&gt;</td>
<td>The role type. Specify one of the following keywords:</td>
</tr>
<tr>
<td>always</td>
<td>Router always translate NSSA-LSA to Type-5 LSA.</td>
</tr>
<tr>
<td>candidate</td>
<td>Router may translate NSSA-LSA to Type-5 LSA if it is elected.</td>
</tr>
<tr>
<td>never</td>
<td>Router never translate NSSA-LSA.</td>
</tr>
</tbody>
</table>
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.

The **no** variant of this command disables this function and restores default behavior.

**Syntax**

```plaintext
area <area-id> range <ip-addr/prefix-length> [advertise|not-advertise]
no area <area-id> range <ip-addr/prefix-length>
```

**Default** The area range is not configured by default. The area range is advertised if it is configured.

**Mode** Router Configuration

**Usage** 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>The OSPF area that you summarizing the routes for. Use one of the following</td>
</tr>
<tr>
<td></td>
<td>formats: This can be entered in either dotted decimal format or normal</td>
</tr>
<tr>
<td></td>
<td>decimal format.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>OSPF Area ID expressed in IPv4 address format A.B.C.D.</td>
</tr>
<tr>
<td>&lt;0-4294967295&gt;</td>
<td>OSPF Area ID expressed as a decimal number within the range shown.</td>
</tr>
</tbody>
</table>

For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.

<table>
<thead>
<tr>
<th>&lt;ip-addr/prefix-length&gt;</th>
<th>The area range prefix and length.</th>
</tr>
</thead>
<tbody>
<tr>
<td>advertise</td>
<td>Advertise this range as a summary route into other areas.</td>
</tr>
<tr>
<td>not-advertise</td>
<td>Does not advertise this range.</td>
</tr>
</tbody>
</table>
OSPF COMMANDS
AREA RANGE

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
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.  
`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**

```plaintext
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] [authentication] [retransmit-interval] [transmit-delay]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>OSPF Area ID expressed in IPv4 address format A.B.C.D.</td>
</tr>
<tr>
<td>&lt;0-4294967295&gt;</td>
<td>OSPF Area ID expressed as a decimal number within the range shown.</td>
</tr>
<tr>
<td></td>
<td>For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>The OSPF router ID of the virtual link neighbor.</td>
</tr>
<tr>
<td>&lt;auth-key&gt;</td>
<td>Specifies the password used for this virtual link. Use the format:</td>
</tr>
<tr>
<td></td>
<td>authentication-key&lt;pswd-short&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;pswd-short&gt;                  An 8 character password.</td>
</tr>
<tr>
<td>&lt;msg-key&gt;</td>
<td>Specifies a message digest key using the MD5 encryption algorithm. Use the following format:</td>
</tr>
<tr>
<td></td>
<td>message-digest-key&lt;1-255&gt; md5&lt;pswd-long&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;1-255&gt;                      The key ID.</td>
</tr>
<tr>
<td></td>
<td>&lt;pswd-long&gt;                  Authentication password of 16 characters.</td>
</tr>
<tr>
<td>authentication</td>
<td>Enables authentication on this virtual link.</td>
</tr>
</tbody>
</table>
### OSPF COMMANDS
### AREA VIRTUAL-LINK

#### 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 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
```bash
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# area 1 virtual-link 10.10.11.50 hello 5 dead 10
```

### Parameter Description Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>message-digest</td>
<td>Use message-digest authentication.</td>
</tr>
<tr>
<td>null</td>
<td>Use null authentication to override password or message digest.</td>
</tr>
<tr>
<td>dead-interval</td>
<td>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</td>
</tr>
<tr>
<td></td>
<td><code>&lt;1-65535&gt;</code> The number of seconds in the interval.</td>
</tr>
<tr>
<td>hello-interval</td>
<td>The interval the router waits before it sends a hello packet. Default: 10 seconds</td>
</tr>
<tr>
<td></td>
<td><code>&lt;1-65535&gt;</code> The number of seconds in the interval.</td>
</tr>
<tr>
<td>retransmit-interval</td>
<td>The interval the router waits before it retransmits a packet. Default: 5 seconds</td>
</tr>
<tr>
<td></td>
<td><code>&lt;1-3600&gt;</code> The number of seconds in the interval.</td>
</tr>
<tr>
<td>transmit-delay</td>
<td>The interval the router waits before it transmits a packet. Default: 1 seconds</td>
</tr>
<tr>
<td></td>
<td><code>&lt;1-3600&gt;</code> The number of seconds in the interval.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4294967&gt;</td>
<td>The reference bandwidth in terms of Mbits per second (Mbps).</td>
</tr>
</tbody>
</table>

**Default**
1000 Mbps

**Usage**
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 the reference bandwidth command.

### Mode
Router Configuration

### Example
```bash
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. 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**
```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# bandwidth 1000000
```

**Related Commands**
- `show running-config`
- `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.

By default, opaque-LSAs are enabled.

Use the **no** variant of this command to disables opaque-LSAs.

**Syntax**

```
capability opaque
no capability opaque
```

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graceful</td>
<td>Enable graceful OSPF restart.</td>
</tr>
<tr>
<td>signaling</td>
<td>Enable OSPF restart signaling.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(&lt;0-65535&gt;)</td>
<td>The Routing Process ID.</td>
</tr>
</tbody>
</table>

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>abr</td>
<td>Shows ABR events.</td>
</tr>
<tr>
<td>asbr</td>
<td>Shows ASBR events.</td>
</tr>
<tr>
<td>lsa</td>
<td>Shows LSA events.</td>
</tr>
<tr>
<td>nssa</td>
<td>Shows NSSA events.</td>
</tr>
<tr>
<td>os</td>
<td>Shows OS interaction events.</td>
</tr>
<tr>
<td>router</td>
<td>Shows other router events.</td>
</tr>
<tr>
<td>vlink</td>
<td>Shows virtual link events.</td>
</tr>
</tbody>
</table>

**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]
```

**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**
```
display ospf lsa [flooding] [generate] [install] [maxage] [refresh]
no display ospf lsa [flooding] [generate] [install] [maxage] [refresh]
```

**Mode**  
Privileged Exec and Global Configuration

**Examples**
```
awplus# undebug ospf lsa refresh
```

**Output**  
Figure 21-1: 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**

```
dump ospf nfsm [events] [status] [timers]
no dump ospf nfsm [events] [status] [timers]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>Displays NFSM event information.</td>
</tr>
<tr>
<td>status</td>
<td>Displays NFSM status information.</td>
</tr>
<tr>
<td>timers</td>
<td>Displays NFSM timer information.</td>
</tr>
</tbody>
</table>

**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**  
d.debug ospf nsm [interface] [redistribute]

no debug ospf nsm [interface] [redistribute]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specify NSM interface information.</td>
</tr>
<tr>
<td>redistribute</td>
<td>Specify NSM redistribute information.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec and Global Configuration

**Examples**

awplus# debug ospf nsm interface

awplus# no debug ospf nsm redistribute

awplus# undebug ospf nsm interface

**Related Commands**

terminal monitor

undebug ospf nsm
**debug ospf packet**

**Overview**
This command enables debugging options for OSPF packets.

To enable all debugging options, specify `debug ospf packet` with no additional parameters.

The `no` and `undebug` variant of this command disable OSPF packet debugging. Use this command without parameters to disable all options.

**Syntax**
```plaintext
dump 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]
```

**Mode**
Privileged Exec and Global Configuration

**Examples**
```plaintext
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dd</td>
<td>Specifies debugging for OSPF database descriptions.</td>
</tr>
<tr>
<td>detail</td>
<td>Sets the debug option to detailed information.</td>
</tr>
<tr>
<td>hello</td>
<td>Specifies debugging for OSPF hello packets.</td>
</tr>
<tr>
<td>ls-ack</td>
<td>Specifies debugging for OSPF link state acknowledgments.</td>
</tr>
<tr>
<td>ls-request</td>
<td>Specifies debugging for OSPF link state requests.</td>
</tr>
<tr>
<td>ls-update</td>
<td>Specifies debugging for OSPF link state updates.</td>
</tr>
<tr>
<td>recv</td>
<td>Specifies the debug option set for received packets.</td>
</tr>
<tr>
<td>send</td>
<td>Specifies the debug option set for sent packets.</td>
</tr>
</tbody>
</table>
**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ia</td>
<td>Specifies the debugging of Inter-Area route calculation.</td>
</tr>
<tr>
<td>ase</td>
<td>Specifies the debugging of external route calculation.</td>
</tr>
<tr>
<td>install</td>
<td>Specifies the debugging of route installation.</td>
</tr>
<tr>
<td>spf</td>
<td>Specifies the debugging of SPF calculation.</td>
</tr>
</tbody>
</table>

**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 (OSPF)

**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). An ASBR does not by default, 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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>always</code></td>
<td>Used to advertise the default route regardless of whether there is a default route.</td>
</tr>
<tr>
<td><code>&lt;metric&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;1-2&gt;</code></td>
<td>External metric type for default routes, either OSPF External Type 1 or Type 2 metrics. Enter the value 1 or 2.</td>
</tr>
<tr>
<td><code>route-map</code></td>
<td>Specifies to use a specific route-map.</td>
</tr>
<tr>
<td><code>&lt;route-map&gt;</code></td>
<td>The route-map name. It is a string comprised of any characters, numbers or symbols.</td>
</tr>
</tbody>
</table>

**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>]
```

**Mode**  
Router Configuration

**Usage**  
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)`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-16777214&gt;</code></td>
<td>Default metric value appropriate for the specified routing protocol.</td>
</tr>
</tbody>
</table>
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**
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:

```plaintext
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:

```plaintext
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 **Route Map 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
no distribute-list <access-list-name> in

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;access-list-name&gt;</td>
<td>Specifies the name of the access list. The access list defines which networks are received and which are suppressed.</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that this applies to incoming advertised routes.</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that this applies to outgoing advertised routes.</td>
</tr>
<tr>
<td>&lt;route-map-name&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>connected</td>
<td>Specify the redistribution of connected routes.</td>
</tr>
<tr>
<td>rip</td>
<td>Specify the redistribution of RIP routes.</td>
</tr>
<tr>
<td>static</td>
<td>Specify the redistribution of static routes.</td>
</tr>
</tbody>
</table>

**Mode**  
Router Configuration

**Usage**  
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 calculation 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
```

### 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:

```plaintext
awplus# configure terminal
awplus(config)# router ospf
awplus(config-router)# enable db-summary-opt
```

To disable OSPF database summary list optimization, use the commands:

```plaintext
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>]
```

**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
```
**OSPF COMMANDS**

**IP OSPF AUTHENTICATION**

---

### 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

```plaintext
ip ospf [<ip-address>] authentication [message-digest|null]
no ip ospf [<ip-address>] authentication
```

#### Mode
Interface Configuration for a VLAN interface.

#### Usage
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.

```plaintext
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`

#### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>The IP address of the interface.</td>
</tr>
<tr>
<td><code>message-digest</code></td>
<td>Use the message digest authentication.</td>
</tr>
<tr>
<td><code>null</code></td>
<td>Use no authentication. It overrides password or message-digest authentication of the interface.</td>
</tr>
</tbody>
</table>
**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>
oip ospf [<ip-address>] authentication-key
```

**Default**
By default, an authentication password is not specified.

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
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
```

**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**  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:

\[
\text{reference bandwidth} / \text{interface bandwidth}
\]

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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>The IPv4 address of the interface, in dotted decimal notation.</td>
</tr>
</tbody>
</table>

**Default**
By default, all outgoing LSAs are flooded to the interface.

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
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
```
OSPF COMMANDS

IP OSPF DEAD-INTERVAL

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>The IPv4 address of the interface, in dotted decimal notation.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>The interval in seconds. Default: 40</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>The IP address of the interface, in dotted decimal notation.</td>
</tr>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>The interval in seconds. Default: 10</td>
</tr>
</tbody>
</table>

**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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>The IPv4 address of the interface, in dotted decimal notation.</td>
</tr>
<tr>
<td>&lt;key-id&gt;</td>
<td>A key ID number specified as an integer between 1 and 255.</td>
</tr>
<tr>
<td>md5</td>
<td>Use the MD5 algorithm.</td>
</tr>
<tr>
<td>&lt;pswd-long&gt;</td>
<td>The OSPF password. This is a string of 1 to 16 characters including spaces.</td>
</tr>
</tbody>
</table>

**Default**
By default, there is no MD5 key registered.

**Mode**
Interface Configuration for a VLAN interface.

**Usage**

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 VLAN interface MTU size as Maximum IP packet size. This command forces OSPF to use the specified value, overriding the actual VLAN 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 VLAN interface.

**Mode**  Interface Configuration for a VLAN interface.

**Usage**  This command allows an administrator to configure the MTU size recognized by the OSPF protocol. It does not configure the MTU settings on the VLAN interface. OSPF will not recognize MTU size configuration changes made to the kernel until the MTU size is updated through the CLI.

**Example**  
```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip ospf mtu 1480
```
**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
```

**Mode**  Interface Configuration for a VLAN interface.

**Usage**  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
```

**Default** The default is the `broadcast` OSPF network type for a VLAN interface.

**Mode** Interface Configuration for a VLAN interface.

**Usage** 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>The IP address of the interface.</td>
</tr>
<tr>
<td><code>&lt;priority&gt;</code></td>
<td><code>&lt;0-255&gt;</code> Specifies the Router Priority of the interface.</td>
</tr>
</tbody>
</table>

**Default**  The router priority for an interface is set to 1 by default.

**Mode**  Interface Configuration for a VLAN interface.

**Usage**  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
```

**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**  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>The IP address of the interface.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Specifies the interval in seconds.</td>
</tr>
</tbody>
</table>

**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)# 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>The IP address of the VLAN interface.</td>
</tr>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>Specifies the time, in seconds, to transmit a link-state update.</td>
</tr>
</tbody>
</table>

**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**  
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
```

**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
```

**Default**
The default for the maximum number of OSPF areas is 4294967294.

**Mode**
Router Configuration

**Usage**
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]
```

**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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;network-address&gt;</code></td>
<td>`{&lt;ip-network/m&gt;</td>
</tr>
<tr>
<td><code>&lt;ip-network/m&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;reverse-mask&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;area-id&gt;</code></td>
<td>`{&lt;ip-addr&gt;</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>OSPF Area ID in IPv4 address format, in the form A.B.C.D.</td>
</tr>
<tr>
<td><code>&lt;0-4294967295&gt;</code></td>
<td>OSPF Area ID as 4 octets unsigned integer value.</td>
</tr>
</tbody>
</table>

**Default**  No network area is configured by default.

**Mode**  Router Configuration

**Usage**  OSPF routing can be enabled per IPv4 subnet. The network address can be defined using either the prefix length or a wildcard mask. A wildcard 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}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco</td>
<td>Specifies an alternative ABR using Cisco implementation (RFC 3509). This is the default ABR type.</td>
</tr>
<tr>
<td>ibm</td>
<td>Specifies an alternative ABR using IBM implementation (RFC 3509).</td>
</tr>
<tr>
<td>standard</td>
<td>Specifies a standard behavior ABR (RFC 2328).</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-1800&gt;</td>
<td>Specifies the grace period in seconds.</td>
</tr>
</tbody>
</table>

**Default**
In the AlliedWare Plus™ OSPF implementation, the default OSPF grace-period is 180 seconds.

**Mode**
Global Configuration

**Usage**
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.

When a master failover happens on a VCStack, the OSPF grace-period will be the longest period between the default value (180 seconds is the default OSPF grace-period) and the configured OSPF grace-period value from this command. So the configured OSPF grace-period value will not be used for a VCStack master failover if it is shorter than the default OSPF grace-period.

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-grace-period</td>
<td>Specify help if received grace-period is less than a specified value.</td>
</tr>
<tr>
<td>&lt;grace-period&gt;</td>
<td>Maximum grace period accepted in seconds in range <code>&lt;1-1800&gt;</code>.</td>
</tr>
<tr>
<td>never</td>
<td>Specify the local policy to never to act as a helper for this feature.</td>
</tr>
<tr>
<td>only-reload</td>
<td>Specify help only on software reloads not software upgrades.</td>
</tr>
<tr>
<td>only-upgrade</td>
<td>Specify help only on software upgrades not software reloads.</td>
</tr>
<tr>
<td>router-id</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;router-id&gt;</td>
<td><code>&lt;A.B.C.D&gt;</code> Specify the OSPF Router ID in dotted decimal format A.B.C.D</td>
</tr>
</tbody>
</table>

**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
```
**OSPF COMMANDS**

**OSPF RESTART HELPER**

### 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**
- `<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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;0-4294967294&gt;</code></td>
<td>The maximum number of LSAs.</td>
</tr>
<tr>
<td><code>hard</code></td>
<td>Shutdown occurs if the number of LSAs exceeds the specified value.</td>
</tr>
<tr>
<td><code>soft</code></td>
<td>Warning message appears if the number of LSAs exceeds the specified value.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;max-lsas&gt;</td>
<td>&lt;0-2147483647&gt; The maximum number of Link State Advertisements (LSAs). Note that this value should be the same on all routers in the AS.</td>
</tr>
<tr>
<td>&lt;recover-time&gt;</td>
<td>&lt;0-65535&gt; 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.</td>
</tr>
</tbody>
</table>

**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>]
```

**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 ospf 100
awplus(config-router)# passive-interface vlan2
```

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 {connected|rip|static} 
{metric|metric-type|route-map|tag}  
no redistribute {connected|rip|static} 
{metric|metric-type|route-map|tag}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>Specifies that this applies to the redistribution of connected routes.</td>
</tr>
<tr>
<td>rip</td>
<td>Specifies that this applies to the redistribution of RIP routes.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies that this applies to the redistribution of static routes.</td>
</tr>
</tbody>
</table>
| metric        | metric `<0-16777214>`  
                             Specifies the external metric.                                      |
| metric-type   | metric-type `{1|2}`  
                             Specifies the external metric-type.                                   |
| route-map     | route-map `WORD`  
                             Specifies name of the route-map.                                         |
| tag           | tag `<0-4294967295>`  
                             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**  
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.
**Example**

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.

**Validation Commands**

- `show ip ospf database external`

**Related Commands**

- `distribute-list (OSPF)`
- `match interface`
- `route-map`
**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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>grace-period</td>
<td>Specify the grace period.</td>
</tr>
<tr>
<td>&lt;1-1800&gt;</td>
<td>The grace period in seconds.</td>
</tr>
</tbody>
</table>

**Default**  
In the AlliedWare Plus™ OSPF implementation, the default OSPF grace-period is 180 seconds.

**Mode**  
Privileged Exec

**Usage**  
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`.

When a master failover happens on a VCStack, the OSPF grace-period will be the longest period between the default value (180 seconds is the default OSPF grace-period) and the configured OSPF grace-period value from this command. So the configured OSPF grace-period value will not be used for a VCStack master failover if it is shorter than the default OSPF grace-period.

**Example**  
```
awplus# copy running-config startup-config
awplus# restart ospf graceful grace-period 200
```

**Related Commands**  
- **ospf restart grace-period**
- **ospf restart helper**
**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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;process-id&gt;</td>
<td>A positive number from 1 to 65535, that is used to define a routing process.</td>
</tr>
</tbody>
</table>

**Default**  No routing process is defined by default.

**Mode**  Global Configuration

**Usage**  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
```

#### 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 display which OSPF debugging options are currently enabled.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
show debugging ospf

**Mode**
User Exec and Privileged Exec

**Example**
awplus# show debugging ospf

**Output**
Figure 21-2: 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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ip ospf
show ip ospf <process-id>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;process-id&gt;</td>
<td><code>&lt;0-65535&gt;</code> 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.</td>
</tr>
</tbody>
</table>

**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 21-1: Example output from the show ip ospf command

<table>
<thead>
<tr>
<th>Route Licence: Route</th>
<th>Limit=0, Allocated=0, Visible=0, Internal=0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Licence: Breach</td>
<td>Current=0, Watermark=0</td>
</tr>
<tr>
<td>Routing Process &quot;ospf 10&quot; with ID 192.168.1.1</td>
<td></td>
</tr>
<tr>
<td>Process uptime is 10 hours 24 minutes</td>
<td></td>
</tr>
<tr>
<td>Process bound to VRF default</td>
<td></td>
</tr>
<tr>
<td>Conforms to RFC2328, and RFC1583 Compatibility flag is disabled</td>
<td></td>
</tr>
<tr>
<td>Supports only single TOS (TOS0) routes</td>
<td></td>
</tr>
<tr>
<td>Supports opaque LSA</td>
<td></td>
</tr>
<tr>
<td>Supports Graceful Restart</td>
<td></td>
</tr>
<tr>
<td>SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs</td>
<td></td>
</tr>
<tr>
<td>Refresh timer 10 secs</td>
<td></td>
</tr>
<tr>
<td>Number of incoming current DD exchange neighbors 0/5</td>
<td></td>
</tr>
<tr>
<td>Number of outgoing current DD exchange neighbors 0/5</td>
<td></td>
</tr>
<tr>
<td>Number of external LSA 0. Checksum 0x000000</td>
<td></td>
</tr>
<tr>
<td>Number of opaque AS LSA 0. Checksum 0x000000</td>
<td></td>
</tr>
<tr>
<td>Number of non-default external LSA 0</td>
<td></td>
</tr>
<tr>
<td>External LSA database is unlimited.</td>
<td></td>
</tr>
<tr>
<td>Number of LSA originated 0</td>
<td></td>
</tr>
<tr>
<td>Number of LSA received 0</td>
<td></td>
</tr>
<tr>
<td>Number of areas attached to this router: 2</td>
<td></td>
</tr>
<tr>
<td>Area 0 (BACKBONE) (Inactive)</td>
<td></td>
</tr>
<tr>
<td>Number of interfaces in this area is 0(0)</td>
<td></td>
</tr>
<tr>
<td>Number of fully adjacent neighbors in this area is 0</td>
<td></td>
</tr>
<tr>
<td>Area has no authentication</td>
<td></td>
</tr>
<tr>
<td>SPF algorithm executed 0 times</td>
<td></td>
</tr>
<tr>
<td>Number of LSA 0. Checksum 0x0000000</td>
<td></td>
</tr>
</tbody>
</table>

| 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 0x0000000 |                                               |

Table 21-2: 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 RFC1583 Compatibility 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 21-3: Parameters in the output of the `show ip ospf` command**

<table>
<thead>
<tr>
<th>Output Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Licence: Route: Limit</td>
<td>The maximum number of OSPF routes which may be used for forwarding.</td>
</tr>
<tr>
<td>Allocate</td>
<td>The current total number of OSPF routes allocated in the OSPF module.</td>
</tr>
<tr>
<td>Visible</td>
<td>The current number of OSPF routes which may be used for forwarding.</td>
</tr>
<tr>
<td>Internal</td>
<td>The number of OSPF internal routes used for calculating paths to ASBRs.</td>
</tr>
<tr>
<td>Number of external LSA</td>
<td>The number of external link-state advertisements</td>
</tr>
<tr>
<td>Number of opaque AS LSA</td>
<td>Number of opaque link-state advertisements</td>
</tr>
</tbody>
</table>

**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 “Controlling “show” Command Output” in 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;process-id&gt;</td>
<td>&lt;0-65535&gt; The ID of the router process for which information will be displayed.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Output**

Figure 21-3: 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 “Controlling “show” Command Output” in 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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;process-id&gt;</td>
<td>&lt;0-65535&gt; The ID of the router process for which information will be displayed.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Displays self-originated link states.</td>
</tr>
<tr>
<td>max-age</td>
<td>Displays LSAs in MaxAge list. It maintains the list of all LSAs in the database which have reached the max-age which is 3600 seconds.</td>
</tr>
<tr>
<td>adv-router</td>
<td>Advertising Router LSA.</td>
</tr>
<tr>
<td>&lt;adv-router-id&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 21-4: 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
```
### OSPF COMMANDS

**SHOW IP OSPF DATABASE**

#### Example

```
awplus# show ip ospf database external 1.2.3.4 self-originate
awplus# show ip ospf database self-originate
```

**Figure 21-5:** Example output from the `show ip ospf database self-originate` command

<table>
<thead>
<tr>
<th>OSPF Router process 100 with ID (10.10.11.50)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Link States (Area 0.0.0.1 [NSSA])</td>
</tr>
<tr>
<td>Link ID</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>10.10.11.50</td>
</tr>
<tr>
<td>Link ID</td>
</tr>
<tr>
<td>67.1.4.217</td>
</tr>
<tr>
<td>Link ID</td>
</tr>
<tr>
<td>67.1.4.217</td>
</tr>
</tbody>
</table>
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ip ospf database asbr-summary [<ip-addr>]
[<self-originate>|<adv-router>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;advrouter&gt;</td>
<td>adv-router &lt;ip-address&gt;</td>
</tr>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>A link state ID, as an IP address.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Displays self-originated link states.</td>
</tr>
</tbody>
</table>

**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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Syntax
show ip ospf database external adv-router[<adv-router-id>]
[自我-originate|adv-router<adv-router-id>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Displays self-originated link states.</td>
</tr>
</tbody>
</table>
| <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 21-6: 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 21-7: 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 “Controlling “show” Command Output” in 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> ]

**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 21-8: 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  
LS age: 1648  
Options: 0x2 (*|-|-|-|-|-|E|-)  
LS Type: network-LSA  
Link State ID: 192.30.30.3 (address of Designated Router)  
Advertising Router: 192.30.30.3  
LS Seq Number: 8000000f  
Checksum: 0xe864  
Length: 32  
Network Mask: /24  
Attached Router: 192.30.30.2  
Attached Router: 192.30.30.3
```
Figure 21-9: 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: 1175
    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: 80000002
    Checksum: 0x0dfb1
    Length: 32
    Network Mask: /24
        Attached Router: 192.20.20.1
        Attached Router: 192.30.30.3
    LS age: 1327
    Options: 0x2 (*|-|-|-|-|E|-)
    LS Type: network-LSA
    Link State ID: 192.20.20.2 (address of Designated Router)
    Advertising Router: 192.20.20.2
    LS Seq Number: 8000000d
    Checksum: 0xbce6
    Length: 32
    Network Mask: /24
        Attached Router: 192.20.20.1
        Attached Router: 192.20.20.2
    LS age: 1278
    Options: 0x2 (*|-|-|-|-|E|-)
    LS Type: network-LSA
    Link State ID: 192.30.30.3 (address of Designated Router)
    Advertising Router: 192.30.30.3
    Advertising Router: 192.30.30.3
    LS Seq Number: 80000001
    Checksum: 0x0556
    Length: 32
    Network Mask: /24
        Attached Router: 192.30.30.2
        Attached Router: 192.30.30.3
    LS age: 1436
    Options: 0x2 (*|-|-|-|-|E|-)
    LS Type: network-LSA
    Link State ID: 192.40.40.2 (address of Designated Router)
    Advertising Router: 192.20.20.2
    LS Seq Number: 800000e
    Checksum: 0xf173
    Length: 32
    Network Mask: /24
        Attached Router: 192.20.20.2
        Attached Router: 192.30.30.2
```
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ip ospf database nssa-external [<ip-address>]
[self-originate|<advrouter>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;advrouter&gt;</td>
<td>adv-router &lt;ip-address&gt;</td>
</tr>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>A link state ID, as an IP address.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Displays self-originated link states.</td>
</tr>
</tbody>
</table>

**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 21-10: 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
--More--
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ip ospf database opaque-area [<ip-address>] [self-originate|<advrouter>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;advrouter&gt;</td>
<td>adv-router &lt;ip-address&gt;</td>
</tr>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>A link state ID, as an IP address.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Displays self-originated link states.</td>
</tr>
</tbody>
</table>

**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 21-11: 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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
```
show ip ospf database opaque-as [<ip-address>] 
[ self-originate | <advrouter> ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;advrouter&gt;</td>
<td>adv-router &lt;ip-address&gt;</td>
</tr>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>A link state ID, as an IP address.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Displays self-originated link states.</td>
</tr>
</tbody>
</table>

**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 21-12: 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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Syntax
show ip ospf database opaque-link [<ip-address>]
[self-originate|<advrouter>]

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 21-13: Example output from the show ip ospf database opaque-link command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;advrouter&gt;</td>
<td>adv-router &lt;ip-address&gt;</td>
</tr>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>A link state ID, as an IP address.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Displays self-originated link states.</td>
</tr>
</tbody>
</table>

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 “Controlling “show” Command Output” in 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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Displays self-originated link states.</td>
</tr>
<tr>
<td>&lt;adv-router-id &gt;</td>
<td>The router ID of the advertising router, in IPv4 address format. Note however, that this no longer represents a real address.</td>
</tr>
</tbody>
</table>

**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 21-14: Example output from the `show ip ospf database router` command

```plaintext
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ip ospf database summary [<ip-address>]
[<self-originate><advrouter>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;advrouter&gt;</td>
<td>adv-router &lt;ip-address&gt;</td>
</tr>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>A link state ID, as an IP address.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Displays self-originated link states.</td>
</tr>
</tbody>
</table>

**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 21-15: 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 21-16: Example output from the `show ip ospf database summary self-originate` command

```plaintext
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
```

```markdown
OSPF COMMANDS

SHOW IP OSPF DATABASE SUMMARY

--

Figure 21-16: 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 21-17: 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)
   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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show ip ospf interface [interface-name]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-name&gt;</td>
<td>The VLAN name, for example vlan3.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Examples**  awplus# show ip ospf interface vlan2

**Output**  Figure 21-18: 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 “Controlling “show” Command Output” in 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 21-19: 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
```
Figure 21-20: Example output from the `show ip ospf <ospf-id> neighbor` command

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead Time</th>
<th>Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.3</td>
<td>50</td>
<td>2-Way/DROther</td>
<td>00:01:59*</td>
<td>192.168.200.3</td>
<td>vlan200</td>
</tr>
</tbody>
</table>

Figure 21-21: 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 vlan5
  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 process ID parameter with this command to display the OSPF routing table for specified instances.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ip ospf [<ospf-id>] route
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ospf-id&gt;</td>
<td>&lt;0-65535&gt; 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.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Examples**
To display the OSPF routing table, use the command:
```
awplus# show ip ospf route
```

**Output**
Figure 21-22: 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 “Controlling “show” Command Output” in 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 21-23: 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 “Controlling “show” Command Output” in 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 21-24: 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>]
```

**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 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:

```plaintext
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:

```plaintext
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# no timers spf exp
```

**Related Commands**  
timers spf exp
**Overview**

This command applies the functionality of the no debug ospf events command.
**Overview**  This command applies the functionality of the no `debug ospf ifsm` command.
**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.
**Overview**  This command applies the functionality of the no `debug ospf nsm` command.
**Overview**  
This command applies the functionality of the no `debug ospf packet` command.
undo debug ospf route

**Overview** This command applies the functionality of the no debug ospf route command.
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 923
- "area authentication ipsec spi" on page 924
- "area default-cost (IPv6 OSPF)" on page 926
- "area encryption ipsec spi esp" on page 927
- "area range (IPv6 OSPF)" on page 930
- "area stub (IPv6 OSPF)" on page 932
- "area virtual-link (IPv6 OSPF)" on page 933
- "area virtual-link authentication ipsec spi" on page 935
- "area virtual-link encryption ipsec spi" on page 937
- "auto-cost reference bandwidth (IPv6 OSPF)" on page 940
- "bandwidth (duplicate)" on page 942
- "clear ipv6 ospf process" on page 943
- "debug ipv6 ospf events" on page 944
- "debug ipv6 ospf ifsm" on page 945
- "debug ipv6 ospf lsa" on page 946
- "debug ipv6 ospf nfsm" on page 947
- "debug ipv6 ospf packet" on page 948
- "debug ipv6 ospf route" on page 949
- "default-metric (IPv6 OSPF)" on page 950
- "distance (IPv6 OSPF)" on page 951
- "distribute-list (IPv6 OSPF)" on page 953
- "ipv6 ospf authentication spi" on page 955
- "ipv6 ospf cost" on page 957
- "ipv6 ospf dead-interval" on page 958
- "ipv6 ospf display route single-line" on page 959
- "ipv6 ospf encryption spi esp" on page 960
- "ipv6 ospf hello-interval" on page 963
- "ipv6 ospf network" on page 964
- "ipv6 ospf priority" on page 965
- "ipv6 ospf retransmit-interval" on page 966
- "ipv6 ospf transmit-delay" on page 967
- "ipv6 router ospf area" on page 968
- "max-concurrent-dd (IPv6 OSPF)" on page 970
- "passive-interface (IPv6 OSPF)" on page 971
- "redistribute (IPv6 OSPF)" on page 972
OSPFv3 FOR IPV6 COMMANDS

• “restart ipv6 ospf graceful” on page 974
• “router ipv6 ospf” on page 975
• “router-id (IPv6 OSPF)” on page 976
• “show debugging ipv6 ospf” on page 977
• “show ipv6 ospf” on page 978
• “show ipv6 ospf database” on page 980
• “show ipv6 ospf database external” on page 982
• “show ipv6 ospf database grace” on page 985
• “show ipv6 ospf database inter-prefix” on page 988
• “show ipv6 ospf database inter-router” on page 991
• “show ipv6 ospf database intra-prefix” on page 994
• “show ipv6 ospf database link” on page 997
• “show ipv6 ospf database network” on page 1000
• “show ipv6 ospf database router” on page 1002
• “show ipv6 ospf interface” on page 1007
• “show ipv6 ospf neighbor” on page 1009
• “show ipv6 ospf route” on page 1011
• “show ipv6 ospf virtual-links” on page 1012
• “summary-address (IPv6 OSPF)” on page 1013
• “timers spf (IPv6 OSPF) (deprecated)” on page 1015
• “timers spf exp (IPv6 OSPF)” on page 1016
• “undebug ipv6 ospf events” on page 1017
• “undebug ipv6 ospf ifsm” on page 1018
• “undebug ipv6 ospf lsa” on page 1019
• “undebug ipv6 ospf nfsm” on page 1020
• “undebug ipv6 ospf packet” on page 1021
• “undebug ipv6 ospf route” on page 1022
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**

code

```plaintext
abr-type {cisco|ibm|standard}
no abr-type {cisco|ibm|standard}
```

desc

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco</td>
<td>Specifies an alternative ABR using Cisco implementation (RFC 3509).</td>
</tr>
<tr>
<td></td>
<td>This is the default ABR type.</td>
</tr>
<tr>
<td>ibm</td>
<td>Specifies an alternative ABR using IBM implementation (RFC 3509).</td>
</tr>
<tr>
<td>standard</td>
<td>Specifies a standard behavior ABR (RFC 2328).</td>
</tr>
</tbody>
</table>

**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**

```plaintext
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>OSPF area-ID expressed in IPv4 address format A.B.C.D.</td>
</tr>
<tr>
<td>&lt;0-4294967295&gt;</td>
<td>OSPF area-ID expressed as a decimal number within the range shown.</td>
</tr>
<tr>
<td>&lt;256-4294967295&gt;</td>
<td>Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.</td>
</tr>
<tr>
<td>md5</td>
<td>Specify the MD5 (Message-Digest 5) hashing algorithm.</td>
</tr>
<tr>
<td>&lt;MD5-key&gt;</td>
<td>Enter an MD5 key containing up to 32 hexadecimal characters.</td>
</tr>
<tr>
<td>sha1</td>
<td>Specify the SHA-1 (Secure Hash Algorithm 1) hashing algorithm.</td>
</tr>
<tr>
<td>&lt;SHA1-key&gt;</td>
<td>Enter an SHA-1 key containing up to 40 hexadecimal characters.</td>
</tr>
</tbody>
</table>

**Mode**

Router Configuration

**Usage**

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, 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 OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 authentication ipsec spi 1000 md5 1234567890ABCDEF1234567890ABCDEF
```

To enable SHA-1 authentication with a 40 hexadecimal character key for OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 authentication ipsec spi 1000 sha1 1234567890ABCDEF1234567890ABCDEF12345678
```

To disable authentication for OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no area 1 authentication ipsec spi 1000
```

Related Commands

- `area encryption ipsec spi esp`
- `area virtual-link authentication ipsec spi`
- `area virtual-link encryption ipsec spi`
- `ipv6 ospf authentication spi`
- `ipv6 ospf encryption spi esp`
- `show ipv6 ospf`
area default-cost (IPv6 OSPF)

**Overview**  This command specifies a cost for the default summary route sent into a stub area. The no variant of this command removes the assigned default-route cost.

**Syntax**  
```
area <area-id> default-cost <0-16777215>
n_area <area-id> default-cost
```

**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>}
```

```
oarea <area-id> encryption ipsec spi <256-4294967295>
```

## Mode

Router Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>&lt;ip-addr&gt; OSPF area-ID expressed in IPv4 address format A.B.C.D.</td>
</tr>
<tr>
<td></td>
<td>&lt;0-4294967295&gt; OSPF area-ID expressed as a decimal number within the range shown.</td>
</tr>
<tr>
<td></td>
<td>For example, the values 0.0.1.2 and decimal 258 would both define the same area-ID.</td>
</tr>
<tr>
<td>&lt;256-4294967295&gt;</td>
<td>Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.</td>
</tr>
<tr>
<td>esp</td>
<td>Specify the esp keyword (Encapsulating Security Payload) to then apply either AES-CBC or 3DES encryption.</td>
</tr>
<tr>
<td>aes-cbc</td>
<td>Specify this keyword to enable AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) encryption.</td>
</tr>
<tr>
<td>&lt;AES-CBC-key&gt;</td>
<td>Enter an AES-CBC key containing either 32, 48, or 64 hexadecimal characters.</td>
</tr>
<tr>
<td>3des</td>
<td>Specify 3DES (Triple Data Encryption Standard) encryption.</td>
</tr>
<tr>
<td>&lt;3DES-key&gt;</td>
<td>Enter a 3DES key containing 48 hexadecimal characters.</td>
</tr>
<tr>
<td>null</td>
<td>Specify ESP without AES-CBC or 3DES encryption applied.</td>
</tr>
<tr>
<td>md5</td>
<td>Specify the MD5 (Message-Digest 5) encryption algorithm.</td>
</tr>
<tr>
<td>&lt;MD5-key&gt;</td>
<td>Enter an MD5 key containing 32 hexadecimal characters.</td>
</tr>
<tr>
<td>sha1</td>
<td>Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.</td>
</tr>
<tr>
<td>&lt;SHA1-key&gt;</td>
<td>Enter an SHA-1 key containing 40 hexadecimal characters.</td>
</tr>
</tbody>
</table>
**Usage**

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, Allied Telesis recommends 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 OSPF area 1, use the commands:

```plaintext
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 encryption ipsec spi 1000 esp 3des 1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF md5 1234567890ABCDEF1234567890ABCDEF
```

To enable ESP encryption with a 32 hexadecimal character AES-CBC key, and a 40 hexadecimal character SHA-1 authentication key for OSPF area 1, use the commands:

```plaintext
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 encryption ipsec spi 1000 esp aes-cbc 1234567890ABCDEF1234567890ABCDEF sha1 1234567890ABCDEF1234567890ABCDEF12345678
```

To disable ESP encryption for OSPF area 1, use the commands:

```plaintext
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]
```
```
o area <area-id> range <ipv6address/prefix-length>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;A.B.C.D&gt;</td>
<td>OSPF area-ID expressed in IPv4 address format A.B.C.D.</td>
</tr>
<tr>
<td>&lt;0-4294967295&gt;</td>
<td>OSPF area-ID expressed as a decimal number within the range shown.</td>
</tr>
<tr>
<td></td>
<td>For example the values 0.0.1.2 and decimal 258 would both define the same area-ID.</td>
</tr>
<tr>
<td>&lt;ipv6address/prefix-length&gt;</td>
<td>The IPv6 address uses the format X::X::X::X:Prefix-Length. The prefix-length is usually set between 0 and 64.</td>
</tr>
<tr>
<td>advertise</td>
<td>Advertise this range as a summary route into other areas.</td>
</tr>
<tr>
<td>not-advertise</td>
<td>Do not advertise this range.</td>
</tr>
</tbody>
</table>

**Default**
The area range is not configured by default. The area range is advertised if it is configured.

**Mode**
Router Configuration

**Usage**
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**  
```plaintext
area <area-id> stub [no-summary]
no area <area-id> stub [no-summary]
```

**Example**  
```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# area 100 stub
```

**Related Commands**  
- area default-cost (IPv6 OSPF)
- **Parameter**  
  - **<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.
  - **no-summary** Stops an ABR from sending summary link advertisements into the stub area.
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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;area-id&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;A.B.C.D&gt;</code></td>
<td>OSPF area-ID, expressed in the IPv4 address format <code>&lt;A.B.C.D&gt;</code>.</td>
</tr>
<tr>
<td><code>&lt;0-4294967295&gt;</code></td>
<td>OSPF area-ID expressed as a decimal number within the range shown.</td>
</tr>
<tr>
<td></td>
<td>For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area-ID.</td>
</tr>
<tr>
<td><code>&lt;router-id&gt;</code></td>
<td>The OSPF router ID of the virtual link neighbor.</td>
</tr>
<tr>
<td><code>dead-interval</code></td>
<td>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</td>
</tr>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>The number of seconds in the interval.</td>
</tr>
<tr>
<td><code>hello-interval</code></td>
<td>The interval the router waits before it sends a hello packet. Default: 10 seconds</td>
</tr>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>The number of seconds in the interval.</td>
</tr>
<tr>
<td><code>retransmit-interval</code></td>
<td>The interval the router waits before it retransmits a packet. Default: 5 seconds</td>
</tr>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>The number of seconds in the interval.</td>
</tr>
</tbody>
</table>
**Mode**  Router Configuration

**Usage**  You can configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these two routers, joined by a virtual link, as if they were connected by an unnumbered point-to-point network. To configure a virtual link, you require:

- The transit area-ID, i.e. the area-ID of the non-backbone area that the two backbone routers are both connected to.
- The corresponding virtual link neighbor’s router ID. To see the router ID use the `show ipv6 ospf` command.

Configure the **hello-interval** to be the same for all routers attached to a common network. A short **hello-interval** results in the router detecting topological changes faster but also an increase in the routing traffic.

The **retransmit-interval** is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The **transmit-delay** is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet, are incremented by this amount. Set the **transmit-delay** to be greater than zero. Also, take into account the transmission and propagation delays for the interface.

**Example**  To configure a virtual link through area 1 to the router with router-ID 10.10.11.50, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# area 1 virtual-link 10.10.11.50 hello 5 dead 10
```

**Related Commands**  `show ipv6 ospf`

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>transmit-delay</td>
<td>The interval the router waits before it transmits a packet. Default: 1 seconds</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>The number of seconds in the interval.</td>
</tr>
</tbody>
</table>
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**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>ip-addr</td>
<td>OSPF area-ID expressed in IPv4 address format A.B.C.D.</td>
</tr>
<tr>
<td>0-4294967295</td>
<td>OSPF area-ID expressed as a decimal number within the range shown.</td>
</tr>
<tr>
<td>virtual-link</td>
<td>Specify a virtual link and its parameters.</td>
</tr>
<tr>
<td>&lt;router-ID&gt;</td>
<td>Enter a router ID associated with a virtual link neighbor in IPv4 address format A.B.C.D.</td>
</tr>
<tr>
<td>authentication</td>
<td>Specify this keyword to enable authentication.</td>
</tr>
<tr>
<td>ipsec</td>
<td>Specify this keyword to use Ipsec authentication.</td>
</tr>
<tr>
<td>spi</td>
<td>Specify this keyword to set the SPI (Security Parameters Index).</td>
</tr>
<tr>
<td>256-4294967295</td>
<td>Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.</td>
</tr>
<tr>
<td>md5</td>
<td>Specify the MD5 (Message-Digest 5) encryption algorithm.</td>
</tr>
<tr>
<td>&lt;MD5-key&gt;</td>
<td>Enter an MD5 key containing 32 hexadecimal characters.</td>
</tr>
<tr>
<td>sha1</td>
<td>Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.</td>
</tr>
<tr>
<td>&lt;SHA1-key&gt;</td>
<td>Enter an SHA-1 key containing 40 hexadecimal characters.</td>
</tr>
</tbody>
</table>

**Mode**
Router Configuration

**Usage**
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 OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1
authentication ipsec spi 1000 md5
1234567890ABCDEF1234567890ABCDEF
```

To enable SHA-1 authentication with a 40 hexadecimal character key for virtual links in OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1
authentication ipsec spi 1000 sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To disable authentication for virtual links in OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no area 1 virtual-link 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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;area-id&gt;</code></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td><code>&lt;ip-addr&gt;</code> OSPF area-ID expressed in IPv4 address format A.B.C.D.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;0-4294967295&gt;</code> 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.</td>
</tr>
<tr>
<td><code>virtual-link</code></td>
<td>Specify a virtual link and its parameters.</td>
</tr>
<tr>
<td><code>&lt;router-ID&gt;</code></td>
<td>Enter a router ID associated with a virtual link neighbor in IPv4 address format A.B.C.D.</td>
</tr>
<tr>
<td><code>encryption</code></td>
<td>Specify this keyword to enable encryption.</td>
</tr>
<tr>
<td><code>ipsec</code></td>
<td>Specify this keyword to use IPsec authentication.</td>
</tr>
<tr>
<td><code>spi</code></td>
<td>Specify this keyword to set the SPI (Security Parameters Index).</td>
</tr>
<tr>
<td><code>&lt;256-4294967295&gt;</code></td>
<td>Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.</td>
</tr>
<tr>
<td><code>esp</code></td>
<td>Specify the esp keyword (Encapsulating Security Payload) to then apply either AES-CBC or 3DES encryption.</td>
</tr>
<tr>
<td><code>aes-cbc</code></td>
<td>Specify this keyword to enable AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) encryption.</td>
</tr>
<tr>
<td><code>&lt;AES-CBC-key&gt;</code></td>
<td>Enter an AES-CBC key containing either 32, 48, or 64 hexadecimal characters.</td>
</tr>
<tr>
<td><code>3des</code></td>
<td>Specify 3DES (Triple Data Encryption Standard) encryption.</td>
</tr>
<tr>
<td><code>&lt;3DES-key&gt;</code></td>
<td>Enter a 3DES key containing 48 hexadecimal characters.</td>
</tr>
</tbody>
</table>
### OSPFv3 for IPv6 Commands

**Area Virtual-Link Encryption IPsec SPI**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>null</td>
<td>Specify ESP without AES-CBC or 3DES encryption applied.</td>
</tr>
<tr>
<td>md5</td>
<td>Specify the MD5 (Message-Digest 5) encryption algorithm.</td>
</tr>
<tr>
<td>&lt;MD5-key&gt;</td>
<td>Enter an MD5 key containing 32 hexadecimal characters.</td>
</tr>
<tr>
<td>sha1</td>
<td>Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.</td>
</tr>
<tr>
<td>&lt;SHA1-key&gt;</td>
<td>Enter an SHA-1 key containing 40 hexadecimal characters.</td>
</tr>
</tbody>
</table>

**Mode**

Router Configuration

**Usage**

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 OSPFV3 area 1, use the commands:

```plaintext
cwplus# configure terminal
cwplus(config)# router ipv6 ospf
cwplus(config-router)# area 1 virtual-link 10.0.0.1 encryption ipsec spi 1000 esp null md5 1234567890ABCDEF1234567890ABCDEF
```
To enable ESP encryption, but not apply an AES-CBC key or a 3DES key, and SHA-1 authentication with a 40 hexadecimal character key for virtual links in OSPF area 1, use the commands:

awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1 encryption ipsec spi 1000 esp null sha1 1234567890ABCDEF1234567890ABCDEF12345678

To enable ESP encryption with a 32 hexadecimal character AES-CBC key and a 40 hexadecimal character SHA-1 authentication key for virtual links in OSPF area 1, use the commands:

awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1 encryption ipsec spi 1000 esp aes-cbc 1234567890ABCDEF1234567890ABCDEF sha1 1234567890ABCDEF1234567890ABCDEF12345678

To enable ESP encryption with a 48 hexadecimal character 3DES key and a 40 hexadecimal character SHA-1 authentication key for virtual links in OSPF area 1, use the commands:

awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1 encryption ipsec spi 1000 esp 3des 1234567890ABCDEF1234567890ABCDEF sha1 1234567890ABCDEF1234567890ABCDEF12345678

To disable authentication for virtual links in OSPF area 1, use the commands:

awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no area 1 virtual-link 10.0.0.1 authentication ipsec spi 1000

**Related Commands**

area authentication ipsec spi
area encryption ipsec spi esp
area virtual-link authentication ipsec spi
show ipv6 ospf virtual-links
auto-cost reference bandwidth (IPv6 OSPF)

**Overview**
This command controls how OSPF calculates default metrics for the interface. Use the `no` variant of this command to assign cost based only on the interface bandwidth.

**Syntax**
```
auto-cost reference-bandwidth <1-4294967>
no auto-cost reference-bandwidth
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-4294967&gt;</code></td>
<td>The reference bandwidth, measured in Mbits per second (Mbps).</td>
</tr>
</tbody>
</table>

**Default**
1000 Mbps

**Usage**
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 (duplicate)` 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 (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 the reference bandwidth command.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Router Configuration</th>
</tr>
</thead>
</table>
| Example | awplus# configure terminal  
awplus(config)# router ipv6 ospf 20  
awplus(config-router)# auto-cost reference-bandwidth 1000 |

**Related Commands**

- `ipv6 ospf cost`
bandwidth (duplicate)

**Overview**
Use this command to specify the maximum bandwidth to be used for each VLAN interface.

The bandwidth value is in bits. 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
```

**Mode**
Interface Configuration for a VLAN interface.

**Example**
```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# bandwidth 1000000
```

**Related Commands**
- `show running-config`
- `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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0–65535&gt;</td>
<td>The routing process ID.</td>
</tr>
</tbody>
</table>

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>abr</td>
<td>Shows ABR events.</td>
</tr>
<tr>
<td>asbr</td>
<td>Shows ASBR events.</td>
</tr>
<tr>
<td>router</td>
<td>Shows other router events.</td>
</tr>
<tr>
<td>os</td>
<td>Shows OS events.</td>
</tr>
<tr>
<td>vlink</td>
<td>Shows virtual link events.</td>
</tr>
</tbody>
</table>

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>Displays IFSM event information.</td>
</tr>
<tr>
<td>status</td>
<td>Displays IFSM status information.</td>
</tr>
<tr>
<td>timers</td>
<td>Displays IFSM timer information.</td>
</tr>
</tbody>
</table>

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flooding</td>
<td>Displays LSA flooding.</td>
</tr>
<tr>
<td>generate</td>
<td>Displays LSA generation.</td>
</tr>
<tr>
<td>install</td>
<td>Show LSA installation.</td>
</tr>
<tr>
<td>maxage</td>
<td>Shows maximum age of the LSA in seconds.</td>
</tr>
<tr>
<td>refresh</td>
<td>Displays LSA refresh.</td>
</tr>
</tbody>
</table>

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>Displays NFSM event information.</td>
</tr>
<tr>
<td>status</td>
<td>Displays NFSM status information.</td>
</tr>
<tr>
<td>timers</td>
<td>Displays NFSM timer information.</td>
</tr>
</tbody>
</table>

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dd</td>
<td>Specifies debugging for IPv6 OSPF database descriptions.</td>
</tr>
<tr>
<td>detail</td>
<td>Sets the debug option to detailed information.</td>
</tr>
<tr>
<td>hello</td>
<td>Specifies debugging for IPv6 OSPF hello packets.</td>
</tr>
<tr>
<td>ls-ack</td>
<td>Specifies debugging for IPv6 OSPF link state acknowledgments.</td>
</tr>
<tr>
<td>ls-request</td>
<td>Specifies debugging for IPv6 OSPF link state requests.</td>
</tr>
<tr>
<td>ls-update</td>
<td>Specifies debugging for IPv6 OSPF link state updates.</td>
</tr>
<tr>
<td>recv</td>
<td>Specifies the debug option set for received packets.</td>
</tr>
<tr>
<td>send</td>
<td>Specifies the debug option set for sent packets.</td>
</tr>
</tbody>
</table>

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ase</td>
<td>Specifies the debugging of external route calculation.</td>
</tr>
<tr>
<td>ia</td>
<td>Specifies the debugging of inter-area route calculation.</td>
</tr>
<tr>
<td>install</td>
<td>Specifies the debugging of route installation.</td>
</tr>
<tr>
<td>spf</td>
<td>Specifies the debugging of SPF calculation.</td>
</tr>
</tbody>
</table>

**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-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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-16777214&gt;</td>
<td>Default metric value appropriate for the specified routing protocol.</td>
</tr>
</tbody>
</table>

**Mode**
Router Configuration

**Usage**
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 Route Selection 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>}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-254&gt;</td>
<td>Specify the Administrative Distance value for OSPFv3 routes.</td>
</tr>
<tr>
<td>external</td>
<td>Sets the distance for routes from other routing domains, learned by redistribution. Specify an OSPFv3 external distance in the range &lt;1-254&gt;.</td>
</tr>
<tr>
<td>inter-area</td>
<td>Sets the distance for all routes from one area to another area. Specify an OSPFv3 inter-area distance in the range &lt;1-254&gt;.</td>
</tr>
<tr>
<td>intra-area</td>
<td>Sets the distance for all routes within an area. Specify an OSPFv3 intra-area distance in the range &lt;1-254&gt;.</td>
</tr>
</tbody>
</table>

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
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 in Router Configuration mode to filter incoming or outgoing OSPFv3 route updates from the networks as defined in an associated access-list.

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 in Router Configuration mode 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}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;access-list&gt;</td>
<td>Specifies the IPv6 access-list number or name to use. The specified access list defines which networks are received and which are suppressed.</td>
</tr>
<tr>
<td>in</td>
<td>Indicates that this applies to incoming advertised routes.</td>
</tr>
<tr>
<td>out</td>
<td>Indicates that this applies to outgoing advertised routes.</td>
</tr>
<tr>
<td>connected</td>
<td>Specify the redistribution of connected routes.</td>
</tr>
<tr>
<td>ospf</td>
<td>Specify the redistribution of OSPFv3 routes.</td>
</tr>
<tr>
<td>&lt;process-tag&gt;</td>
<td>Optionally specify an OSPFv3 process tag for OSPFv3 routes.</td>
</tr>
<tr>
<td>rip</td>
<td>Specify the redistribution of RIPng routes.</td>
</tr>
<tr>
<td>static</td>
<td>Specify the redistribution of connected routes.</td>
</tr>
</tbody>
</table>

Default
Disabled

Mode
Router Configuration

Usage
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)
OSPFv3 FOR IPV6 COMMANDS
IPV6 OSPF AUTHENTICATION SPI

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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication</td>
<td>Specify this keyword to enable authentication.</td>
</tr>
<tr>
<td>ipsec</td>
<td>Specify this keyword to use IPsec authentication.</td>
</tr>
<tr>
<td>spi</td>
<td>Specify this keyword to set the SPI (Security Parameters Index).</td>
</tr>
<tr>
<td>&lt;256-4294967295&gt;</td>
<td>Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.</td>
</tr>
<tr>
<td>md5</td>
<td>Specify the MD5 (Message-Digest 5) hashing algorithm.</td>
</tr>
<tr>
<td>&lt;MD5-key&gt;</td>
<td>Enter an MD5 key containing up to 32 hexadecimal characters.</td>
</tr>
<tr>
<td>sha1</td>
<td>Specify the SHA-1 (Secure Hash Algorithm 1) hashing algorithm.</td>
</tr>
<tr>
<td>&lt;SHA1-key&gt;</td>
<td>Enter an SHA-1 key containing up to 40 hexadecimal characters.</td>
</tr>
<tr>
<td>null</td>
<td>Specify no authentication is applied when no other parameters are applied after this keyword (<code>ipv6 ospf authentication null</code>). Note this overrides any existing area authentication configured.</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration

**Default**
Authentication is not configured on an interface by default.

**Usage**
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.
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 32 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 ipsec 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) command.

Mode
Interface Configuration for a VLAN interface.

Usage
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 auto-cost reference bandwidth (IPv6 OSPF) command.

The interface bandwidth is set by default to 1000000 kbps (or 1000 Mbps), but can be changed by the bandwidth (duplicate) 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 (duplicate)
**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
```

**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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;256-4294967295&gt;</td>
<td>Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.</td>
</tr>
<tr>
<td>esp</td>
<td>Specify the esp keyword (Encapsulating Security Payload) to then apply either AES-CBC or 3DES encryption.</td>
</tr>
<tr>
<td>aes-cbc</td>
<td>Specify this keyword to enable AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) encryption.</td>
</tr>
<tr>
<td>&lt;AES-CBC-key&gt;</td>
<td>Enter an AES-CBC key containing either 32, 48, or 64 hexadecimal characters.</td>
</tr>
<tr>
<td>3des</td>
<td>Specify 3DES (Triple Data Encryption Standard) encryption.</td>
</tr>
<tr>
<td>&lt;3DES-key&gt;</td>
<td>Enter a 3DES key containing 48 hexadecimal characters.</td>
</tr>
<tr>
<td>null</td>
<td>Specify ESP without AES-CBC or 3DES encryption applied.</td>
</tr>
<tr>
<td>md5</td>
<td>Specify the MD5 (Message-Digest 5) encryption algorithm.</td>
</tr>
<tr>
<td>&lt;MD5-key&gt;</td>
<td>Enter an MD5 key containing 32 hexadecimal characters.</td>
</tr>
<tr>
<td>sha1</td>
<td>Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.</td>
</tr>
<tr>
<td>&lt;SHA1-key&gt;</td>
<td>Enter an SHA-1 key containing 40 hexadecimal characters.</td>
</tr>
<tr>
<td>null</td>
<td>Specify no encryption is applied when no other parameters are applied after this keyword (<code>ipv6 ospf encryption null</code>).</td>
</tr>
</tbody>
</table>

**Default**
Authentication is not configured on an interface by default.

**Mode**
Interface Configuration

**Usage**
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
1234567890ABCD1234567890ABCD1234567890ABCD md5
1234567890ABCD1234567890ABCD1234567890ABCD

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 1234567890ABCD1234567890ABCD1234567890ABCD sha1
1234567890ABCD1234567890ABCD1234567890ABCD12345678

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
```

**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 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>Sets the network type to broadcast.</td>
</tr>
<tr>
<td>non-broadcast</td>
<td>Sets the network type to NBMA.</td>
</tr>
<tr>
<td>point-to-multipoint</td>
<td>Sets the network type to point-to-multipoint.</td>
</tr>
<tr>
<td>point-to-point</td>
<td>Sets the network type to point-to-point.</td>
</tr>
</tbody>
</table>

**Default**  
The default is the **broadcast** OSPF network type for a VLAN interface.

**Mode**  
Interface Configuration for a VLAN interface.

**Usage**  
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**:

```bash
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;priority&gt;</code></td>
<td><code>&lt;0-255&gt;</code></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

- **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
```

**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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Specifies the time, in seconds, to transmit a link-state update.</td>
</tr>
</tbody>
</table>
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>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• area-id &lt;A.B.C.D&gt; where A.B.C.D is a number entered in IPv4 address format.</td>
</tr>
<tr>
<td></td>
<td>• area-id &lt;0 to 4294967295&gt;.</td>
</tr>
<tr>
<td>&lt;process-id&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;instance-id&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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**  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
```

**Mode**
Router Configuration

**Usage**
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>]
```

**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>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;protocol&gt;</td>
<td>The routing protocol to be redistributed, can be one of:</td>
</tr>
<tr>
<td>connected</td>
<td>Connected routes</td>
</tr>
<tr>
<td>rip</td>
<td>Routing Internet Protocol</td>
</tr>
<tr>
<td>static</td>
<td>Static Routes</td>
</tr>
<tr>
<td>metric</td>
<td>&lt;0-16777214&gt; Specifies the external metric.</td>
</tr>
<tr>
<td>metric-type</td>
<td>Specifies the external metric-type, either type 1 or type 2.</td>
</tr>
<tr>
<td>route-map</td>
<td>&lt;route-map-entry&gt; Where the route-map-entry specifies the pointer to the specific route-map.</td>
</tr>
</tbody>
</table>

**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**
IPv6 OSPF advertises routes learned from the RIP routing protocol including static or connected routes. Each injected prefix is put into the AS-external-LSA with a specified metric and metric type.

See the **OSPFv3 Feature Overview and Configuration Guide** for more information and examples.
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.

```plaintext
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**
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**  
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

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;router-id&gt;</td>
<td>Specifies the router ID in IPv4 address format.</td>
</tr>
</tbody>
</table>
**show debugging ipv6 ospf**

**Overview**  Use this command in User Exec or Privileged Exec modes to display which OSPFv3 debugging options are currently enabled.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show debugging ipv6 ospf

**Mode**  User Exec and Privileged Exec

**Example**  awplus# show debugging ipv6 ospf

**Output**  Figure 22-1: 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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**

```
show ipv6 ospf
show ipv6 ospf <process-id>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;process-id&gt;</td>
<td>&lt;0-65535&gt; 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.</td>
</tr>
</tbody>
</table>

**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
```
**OSPFv3 for IPv6 Commands**

**SHOW IPV6 OSPF**

**Output**  
Figure 22-2: 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 “Controlling “show” Command Output” in 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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| <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 22-3: Example output from the **show ipv6 ospf P10 database** command
### OSPFv3 Router with ID (0.0.1.1) (Process P10)

#### Link-LSA (Interface vlan2)

<table>
<thead>
<tr>
<th>Link State ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>CkSum</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.202</td>
<td>0.0.1.1</td>
<td>46</td>
<td>0x800000c3</td>
<td>0x5f50</td>
<td>1</td>
</tr>
<tr>
<td>0.0.0.202</td>
<td>0.0.1.2</td>
<td>8</td>
<td>0x800000c3</td>
<td>0x4ca0</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Link-LSA (Interface vlan3)

<table>
<thead>
<tr>
<th>Link State ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>CkSum</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.203</td>
<td>0.0.1.1</td>
<td>1071</td>
<td>0x8000000e</td>
<td>0xe082</td>
<td>1</td>
</tr>
<tr>
<td>0.0.0.203</td>
<td>0.0.1.3</td>
<td>1057</td>
<td>0x8000000e</td>
<td>0xb8aa</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Router-LSA (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link State ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>CkSum</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.1.1</td>
<td>1016</td>
<td>0x800000cd</td>
<td>0xa426</td>
<td>2</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0.0.1.2</td>
<td>979</td>
<td>0x800000d8</td>
<td>0xad2b</td>
<td>1</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0.0.1.3</td>
<td>1005</td>
<td>0x800000cf</td>
<td>0xefed</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Network-LSA (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link State ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>CkSum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.202</td>
<td>0.0.1.2</td>
<td>1764</td>
<td>0x800000c2</td>
<td>0x94c3</td>
</tr>
<tr>
<td>0.0.0.203</td>
<td>0.0.1.3</td>
<td>1010</td>
<td>0x800000c4</td>
<td>0x8ac8</td>
</tr>
</tbody>
</table>

#### Intra-Area-Prefix-LSA (Area 0.0.0.0)

<table>
<thead>
<tr>
<th>Link State ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>CkSum</th>
<th>Prefix</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.2</td>
<td>0.0.1.2</td>
<td>978</td>
<td>0x800000a1</td>
<td>0x699a</td>
<td>Router-LSA</td>
<td></td>
</tr>
<tr>
<td>0.0.0.4</td>
<td>0.0.1.2</td>
<td>1764</td>
<td>0x800000c2</td>
<td>0xca4d</td>
<td>Network-LSA</td>
<td></td>
</tr>
<tr>
<td>0.0.0.1</td>
<td>0.0.1.3</td>
<td>1004</td>
<td>0x80000012</td>
<td>0xaee2</td>
<td>Router-LSA</td>
<td></td>
</tr>
<tr>
<td>0.0.0.7</td>
<td>0.0.1.3</td>
<td>1005</td>
<td>0x8000000e</td>
<td>0x3c89</td>
<td>Network-LSA</td>
<td></td>
</tr>
</tbody>
</table>

#### AS-external-LSA

<table>
<thead>
<tr>
<th>Link State ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>CkSum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.13</td>
<td>0.0.1.1</td>
<td>1071</td>
<td>0x8000000e</td>
<td>0xca9f</td>
</tr>
<tr>
<td>0.0.0.14</td>
<td>0.0.1.1</td>
<td>1071</td>
<td>0x8000000e</td>
<td>0xcc9b</td>
</tr>
<tr>
<td>0.0.0.15</td>
<td>0.0.1.1</td>
<td>1071</td>
<td>0x8000000e</td>
<td>0xce97</td>
</tr>
<tr>
<td>0.0.0.16</td>
<td>0.0.1.1</td>
<td>1071</td>
<td>0x8000000e</td>
<td>0xd093</td>
</tr>
<tr>
<td>0.0.0.17</td>
<td>0.0.1.1</td>
<td>1071</td>
<td>0x8000000e</td>
<td>0xd28f</td>
</tr>
<tr>
<td>0.0.0.18</td>
<td>0.0.1.1</td>
<td>1071</td>
<td>0x8000000e</td>
<td>0xd48b</td>
</tr>
</tbody>
</table>
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 “Controlling “show” Command Output” in 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>]

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 22-4: Example output from the show ipv6 ospf database external command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;adv-router-id&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>self originate</td>
<td>Self-originated link states.</td>
</tr>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
</tbody>
</table>

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 EXTERNAL**

**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
OSPFv3 FOR IPV6 COMMANDS
SHOWNV6 OSPF DATABASE EXTERNAL

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 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 “Controlling “show” Command Output” in 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:

```plaintext
awplus# show ipv6 ospf database grace adv-router 10.10.10.1
```

**Output**  
Figure 22-5: 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
```
### OSPFV3 for IPv6 Commands

#### Show IPv6 OSPF Database Grace

| LS age: 1087 | LS Type: AS-External-LSA |
| LS Seq Number: 0x8000000C | Advertising Router: 0.0.1.1 |
| Advertising Router: 0.0.1.1 | Link State ID: 0.0.0.14 |
| Link State ID: 0.0.0.14 | LS Seq Number: 0x8000000C |
| LS Seq Number: 0x8000000C | Advertising Router: 0.0.1.1 |
| Advertising Router: 0.0.1.1 | Link State ID: 0.0.0.15 |
| Link State ID: 0.0.0.15 | LS Seq Number: 0x8000000C |
| LS Seq Number: 0x8000000C | Advertising Router: 0.0.1.1 |
| Advertising Router: 0.0.1.1 | Link State ID: 0.0.0.16 |
| Link State ID: 0.0.0.16 | LS Seq Number: 0x8000000C |
| LS Seq Number: 0x8000000C | Advertising Router: 0.0.1.1 |

**Checksum:**
- 0xD099
- 0xD295
- 0xD491

**Length:**
- 52

**Metric Type:**
- 2 (Larger than any link state path)

**Metric:**
- 20

**Prefix:**
- 2011:2222::/64
- 2012:2222::/64
- 2013:2222::/64

**Prefix Options:**
- 0 (-|-|-|-)

**Forwarding Address:**
- 2003:1111::1

---

**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

---

**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

---

**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
### OSPFv3 for IPv6 Commands

#### SHOW IPV6 OSPF DATABASE GRACE

<table>
<thead>
<tr>
<th>LS age: 1087</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LS Type:</strong> AS-External-LSA</td>
</tr>
<tr>
<td><strong>Link State ID:</strong> 0.0.0.17</td>
</tr>
<tr>
<td><strong>Advertising Router:</strong> 0.0.1.1</td>
</tr>
<tr>
<td><strong>LS Seq Number:</strong> 0x8000000C</td>
</tr>
<tr>
<td><strong>Checksum:</strong> 0xD68D</td>
</tr>
<tr>
<td><strong>Length:</strong> 52</td>
</tr>
<tr>
<td><strong>Metric Type:</strong> 2 (Larger than any link state path)</td>
</tr>
<tr>
<td><strong>Metric:</strong> 20</td>
</tr>
<tr>
<td><strong>Prefix:</strong> 2014:2222::/64</td>
</tr>
<tr>
<td><strong>Prefix Options:</strong> 0 (-</td>
</tr>
<tr>
<td><strong>Forwarding Address:</strong> 2003:1111::1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LS age: 1087</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LS Type:</strong> AS-External-LSA</td>
</tr>
<tr>
<td><strong>Link State ID:</strong> 0.0.0.18</td>
</tr>
<tr>
<td><strong>Advertising Router:</strong> 0.0.1.1</td>
</tr>
<tr>
<td><strong>LS Seq Number:</strong> 0x8000000C</td>
</tr>
<tr>
<td><strong>Checksum:</strong> 0xD889</td>
</tr>
<tr>
<td><strong>Length:</strong> 52</td>
</tr>
<tr>
<td><strong>Metric Type:</strong> 2 (Larger than any link state path)</td>
</tr>
<tr>
<td><strong>Metric:</strong> 20</td>
</tr>
<tr>
<td><strong>Prefix:</strong> 2015:2222::/64</td>
</tr>
<tr>
<td><strong>Prefix Options:</strong> 0 (-</td>
</tr>
<tr>
<td><strong>Forwarding Address:</strong> 2003:1111::1</td>
</tr>
</tbody>
</table>
**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 “Controlling “show” Command Output” in 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>]
```

**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 22-6: Example output from the show ipv6 ospf database inter-prefix command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;adv-router-id&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>self originate</td>
<td>Self-originated link states.</td>
</tr>
</tbody>
</table>

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
```
### OSPFv3 for IPv6 Commands

**SHOW IPv6 OSPF DATABASE INTER-PREFIX**

<table>
<thead>
<tr>
<th>LS age</th>
<th>LS Type</th>
<th>Link State ID</th>
<th>Advertising Router</th>
<th>LS Seq Number</th>
<th>Checksum</th>
<th>Length</th>
<th>Metric Type</th>
<th>Metric</th>
<th>Prefix</th>
<th>Prefix Options</th>
<th>Forwarding Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1087</td>
<td>AS-External-LSA</td>
<td>0.0.0.14</td>
<td>0.0.1.1</td>
<td>0x8000000C</td>
<td>0xD099</td>
<td>52</td>
<td>Larger than any link state path</td>
<td>20</td>
<td>2011:2222::/64</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1087</td>
<td>AS-External-LSA</td>
<td>0.0.0.15</td>
<td>0.0.1.1</td>
<td>0x8000000C</td>
<td>0xD295</td>
<td>52</td>
<td>Larger than any link state path</td>
<td>20</td>
<td>2012:2222::/64</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1087</td>
<td>AS-External-LSA</td>
<td>0.0.0.16</td>
<td>0.0.1.1</td>
<td>0x8000000C</td>
<td>0xD491</td>
<td>52</td>
<td>Larger than any link state path</td>
<td>20</td>
<td>2013:2222::/64</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
**SHOW IPV6 OSPF DATABASE INTER-PREFIX**

```
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 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 “Controlling “show” Command Output” in 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>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;adv-router-id&gt;</code></td>
<td>The Advertising Router ID (usually entered in IPv4 address format A.B.C.D).</td>
</tr>
<tr>
<td></td>
<td>Note that this ID component no longer represents an address; it is simply a</td>
</tr>
<tr>
<td></td>
<td>character string that has an IPv4 address format.</td>
</tr>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>self originate</td>
<td>Self-originated link states.</td>
</tr>
</tbody>
</table>

**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 22-7: 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
```
<table>
<thead>
<tr>
<th>LS age: 1087</th>
<th>LS age: 1087</th>
<th>LS age: 1087</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Type: AS-External-LSA</td>
<td>LS Type: AS-External-LSA</td>
<td>LS Type: AS-External-LSA</td>
</tr>
<tr>
<td>Link State ID: 0.0.0.14</td>
<td>Link State ID: 0.0.0.15</td>
<td>Link State ID: 0.0.0.16</td>
</tr>
<tr>
<td>Advertising Router: 0.0.1.1</td>
<td>Advertising Router: 0.0.1.1</td>
<td>Advertising Router: 0.0.1.1</td>
</tr>
<tr>
<td>LS Seq Number: 0x8000000C</td>
<td>LS Seq Number: 0x8000000C</td>
<td>LS Seq Number: 0x8000000C</td>
</tr>
<tr>
<td>Checksum: 0xD099</td>
<td>Checksum: 0xD295</td>
<td>Checksum: 0xD491</td>
</tr>
<tr>
<td>Length: 52</td>
<td>Length: 52</td>
<td>Length: 52</td>
</tr>
<tr>
<td>Metric Type: 2 (Larger than any link state path)</td>
<td>Metric Type: 2 (Larger than any link state path)</td>
<td>Metric Type: 2 (Larger than any link state path)</td>
</tr>
<tr>
<td>Metric: 20</td>
<td>Metric: 20</td>
<td>Metric: 20</td>
</tr>
<tr>
<td>Prefix: 2011:2222::/64</td>
<td>Prefix: 2012:2222::/64</td>
<td>Prefix: 2013:2222::/64</td>
</tr>
<tr>
<td>Prefix Options: 0 (-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Forwarding Address: 2003:1111::1</td>
<td>Forwarding Address: 2003:1111::1</td>
<td>Forwarding Address: 2003:1111::1</td>
</tr>
</tbody>
</table>
OSPFV3 FOR IPV6 COMMANDS
SHOW IPV6 OSPF DATABASE INTER-ROUTER

```
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 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 “Controlling “show” Command Output” in 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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;adv-router-id&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>self originate</td>
<td>Self-originated link states.</td>
</tr>
</tbody>
</table>

**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 22-8: 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
```
OSPFv3 for IPv6 Commands
SHOW IPV6 OSPF DATABASE INTRA-PREFIX

<table>
<thead>
<tr>
<th>LS age: 1087</th>
<th>LS Type: AS-External-LSA</th>
<th>Link State ID: 0.0.0.14</th>
<th>Advertising Router: 0.0.1.1</th>
<th>LS Seq Number: 0x8000000C</th>
<th>Checksum: 0xD099</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Length: 52</td>
<td>Metric Type: 2 (Larger than any link state path)</td>
<td>Metric: 20</td>
<td>Prefix: 2011:2222::/64</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Prefix Options: 0 (-</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LS age: 1087</th>
<th>LS Type: AS-External-LSA</th>
<th>Link State ID: 0.0.0.15</th>
<th>Advertising Router: 0.0.1.1</th>
<th>LS Seq Number: 0x8000000C</th>
<th>Checksum: 0xD295</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Length: 52</td>
<td>Metric Type: 2 (Larger than any link state path)</td>
<td>Metric: 20</td>
<td>Prefix: 2012:2222::/64</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Prefix Options: 0 (-</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LS age: 1087</th>
<th>LS Type: AS-External-LSA</th>
<th>Link State ID: 0.0.0.16</th>
<th>Advertising Router: 0.0.1.1</th>
<th>LS Seq Number: 0x8000000C</th>
<th>Checksum: 0xD491</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Length: 52</td>
<td>Metric Type: 2 (Larger than any link state path)</td>
<td>Metric: 20</td>
<td>Prefix: 2013:2222::/64</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Prefix Options: 0 (-</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>
### OSPFV3 for IPv6 Commands

#### SHOW IPV6 OSPF DATABASE INTRA-PREFIX

<table>
<thead>
<tr>
<th>LS age: 1087</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Type: AS-External-LSA</td>
</tr>
<tr>
<td>Link State ID: 0.0.0.17</td>
</tr>
<tr>
<td>Advertising Router: 0.0.1.1</td>
</tr>
<tr>
<td>LS Seq Number: 0x8000000C</td>
</tr>
<tr>
<td>Checksum: 0xD68D</td>
</tr>
<tr>
<td>Length: 52</td>
</tr>
<tr>
<td>Metric Type: 2 (Larger than any link state path)</td>
</tr>
<tr>
<td>Metric: 20</td>
</tr>
<tr>
<td>Prefix: 2014:2222::/64</td>
</tr>
<tr>
<td>Prefix Options: 0 (-</td>
</tr>
<tr>
<td>Forwarding Address: 2003:1111::1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LS age: 1087</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Type: AS-External-LSA</td>
</tr>
<tr>
<td>Link State ID: 0.0.0.18</td>
</tr>
<tr>
<td>Advertising Router: 0.0.1.1</td>
</tr>
<tr>
<td>LS Seq Number: 0x8000000C</td>
</tr>
<tr>
<td>Checksum: 0xD889</td>
</tr>
<tr>
<td>Length: 52</td>
</tr>
<tr>
<td>Metric Type: 2 (Larger than any link state path)</td>
</tr>
<tr>
<td>Metric: 20</td>
</tr>
<tr>
<td>Prefix: 2015:2222::/64</td>
</tr>
<tr>
<td>Prefix Options: 0 (-</td>
</tr>
<tr>
<td>Forwarding Address: 2003:1111::1</td>
</tr>
</tbody>
</table>
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 “Controlling “show” Command Output” in 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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;adv-router-id&gt;</td>
<td>The Advertising Router ID (usually entered in IPv4 address format A.B.C.D).</td>
</tr>
<tr>
<td></td>
<td>Note that this ID component no longer represents an address; it is simply a</td>
</tr>
<tr>
<td></td>
<td>character string that has an IPv4 address format.</td>
</tr>
<tr>
<td>adv-router</td>
<td>Displays all the LSAs of the specified router.</td>
</tr>
<tr>
<td>self originate</td>
<td>Self-originated link states.</td>
</tr>
</tbody>
</table>

**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 22-9: Example output from the show ipv6 ospf database link command

```
LS age: 1087  
LS Type: AS-External-LSA  
Link State ID: 0.0.0.13  
Advertising Router: 0.0.1.1  
LS Seq Number: 0x8000000C  
Checksum: 0xCE9D  
Length: 52  
Metric Type: 2 (Larger than any link state path)  
Metric: 20  
Prefix: 2010:2222::/64  
Prefix Options: 0 (-|-|-|-)  
Forwarding Address: 2003:1111::1
```
**OSPFv3 for IPv6 Commands**

**SHOW IPV6 OSPF DATABASE LINK**

| 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 |
SHOW IPV6 OSPF DATABASE LINK

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 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 “Controlling “show” Command Output” in 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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;adv-router-id&gt;</td>
<td>The router ID of the advertising router, in IPv4 address format. Note, however, that this no longer represents a real address.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Self-originated link states.</td>
</tr>
<tr>
<td>adv-router</td>
<td>The advertising router selected.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Examples**  To display information about the OSPFv3 network LSAs, use the following command:

```bash
awplus# show ipv6 ospf database network
```
### OSPFv3 FOR IPv6 COMMANDS

**SHOW IPv6 OSPF DATABASE NETWORK**

**Output**  
Figure 22-10: Example output from the `show ipv6 ospf database network` command

<table>
<thead>
<tr>
<th>OSPFv3 Router with ID (0.0.1.1) (Process P10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network-LSA (Area 0.0.0.0)</td>
</tr>
<tr>
<td>LS age: 97</td>
</tr>
<tr>
<td>LS Type: Network-LSA</td>
</tr>
<tr>
<td>Link State ID: 0.0.0.202</td>
</tr>
<tr>
<td>Advertising Router: 0.0.1.2</td>
</tr>
<tr>
<td>LS Seq Number: 0x800000C3</td>
</tr>
<tr>
<td>Checksum: 0x92C4</td>
</tr>
<tr>
<td>Length: 32</td>
</tr>
<tr>
<td>Options: 0x000013 (-</td>
</tr>
<tr>
<td>Attached Router: 0.0.1.2</td>
</tr>
<tr>
<td>Attached Router: 0.0.1.1</td>
</tr>
</tbody>
</table>

| 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 “Controlling “show” Command Output” in 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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;adv-router-id&gt;</td>
<td>The router ID of the advertising router, in IPv4 address format.</td>
</tr>
<tr>
<td></td>
<td>Note, however, that this no longer represents a real address.</td>
</tr>
<tr>
<td>self-originate</td>
<td>Self-originated link states.</td>
</tr>
<tr>
<td>adv-router</td>
<td>The advertising router selected.</td>
</tr>
</tbody>
</table>

**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 22-11: Example output from the show ipv6 ospf database router command

<table>
<thead>
<tr>
<th>OSPFv3 Router with ID (0.0.1.3) (Process P10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router-LSA (Area 0.0.0.0)</td>
</tr>
<tr>
<td>LS age: 556</td>
</tr>
<tr>
<td>LS Type: Router-LSA</td>
</tr>
<tr>
<td>Link State ID: 0.0.0.0</td>
</tr>
<tr>
<td>Advertising Router: 0.0.1.1</td>
</tr>
<tr>
<td>LS Seq Number: 0x8000000CA</td>
</tr>
<tr>
<td>Checksum: 0xAA23</td>
</tr>
<tr>
<td>Length: 56</td>
</tr>
<tr>
<td>Flags: 0x02 (-</td>
</tr>
<tr>
<td>Options: 0x000013 (-</td>
</tr>
<tr>
<td>Link connected to: a Transit Network</td>
</tr>
<tr>
<td>Metric: 1</td>
</tr>
<tr>
<td>Interface ID: 203</td>
</tr>
<tr>
<td>Neighbor Interface ID: 203</td>
</tr>
<tr>
<td>Neighbor Router ID: 0.0.1.3</td>
</tr>
</tbody>
</table>

| 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: 0x8000000D5                     |
| 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                   |

| Link connected to: a Transit Network          |
| Metric: 1                                     |
| Interface ID: 202                             |
| Neighbor Interface ID: 202                    |
| Neighbor Router ID: 0.0.1.2                   |
### OSPFV3 for IPv6 Commands

**SHOW IPV6 OSPF DATABASE ROUTER**

<table>
<thead>
<tr>
<th>LS age</th>
<th>LS Type</th>
<th>Link State ID</th>
<th>Advertising Router</th>
<th>LS Seq Number</th>
<th>Checksum</th>
<th>Length</th>
<th>Flags</th>
<th>Options</th>
<th>Metric Type</th>
<th>Metric</th>
<th>Prefix</th>
<th>Prefix Options</th>
<th>Forwarding Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>543</td>
<td>Router-LSA</td>
<td>0.0.0.0</td>
<td>0.0.1.3</td>
<td>0x8000000CC</td>
<td>0xFD5EA</td>
<td>40</td>
<td>0x00</td>
<td>0x0000013</td>
<td>(-</td>
<td>-</td>
<td>-</td>
<td>-)</td>
<td>0xF5EA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AS-external-LSA</td>
<td>0.0.0.0</td>
<td>0.0.1.3</td>
<td>0x80000009</td>
<td>0xD49A</td>
<td>52</td>
<td>0x00</td>
<td>0x00000009</td>
<td>20</td>
<td>0xD49A</td>
<td>2010:2222::/64</td>
<td>0 (-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AS-external-LSA</td>
<td>0.0.0.0</td>
<td>0.0.1.3</td>
<td>0x80000009</td>
<td>0xD696</td>
<td>52</td>
<td>0x00</td>
<td>0x00000009</td>
<td>20</td>
<td>0xD696</td>
<td>2011:2222::/64</td>
<td>0 (-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AS-external-LSA</td>
<td>0.0.0.0</td>
<td>0.0.1.3</td>
<td>0x80000009</td>
<td>0xD892</td>
<td>52</td>
<td>0x00</td>
<td>0x00000009</td>
<td>20</td>
<td>0xD892</td>
<td>2012:2222::/64</td>
<td>0 (-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SHOW IPV6 OSPF DATABASE ROUTER

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
OSPFv3 FOR IPV6 COMMANDS
SHOW IPV6 OSPF DATABASE ROUTER

| 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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Syntax
show ipv6 ospf interface [<interface-name>]

Mode
User Exec and Privileged Exec

Examples
awplus# show ipv6 ospf interface vlan2

Output
Figure 22-12: 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:fe9e: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 22-13: Example output from the `show ipv6 ospf interface` vlan3 command**

```plaintext
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 “Controlling “show” Command Output” in 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;process-id&gt;</td>
<td><code>&lt;character string&gt;</code> The ID of the OSPF process for which information will be displayed.</td>
</tr>
<tr>
<td>&lt;neighbor-id&gt;</td>
<td>The Neighbor ID, entered in IP address (A.B.C.D) format.</td>
</tr>
<tr>
<td>detail</td>
<td>Detail of all neighbors.</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>IP address of the interface.</td>
</tr>
</tbody>
</table>

**Mode**

User Exec and Privileged Exec

**Examples**

```
awplus# show ipv6 ospf neighbor
```

**Output**

Figure 22-14: Example output from the `show ipv6 ospf neighbor` command

```
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 22-15: Example output from the **show ipv6 ospf neighbor detail** command

```
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Syntax
show ipv6 ospf [<process-id>] route

Mode
User Exec and Privileged Exec

Examples
To display the OSPF routing table, use the command:

awplus# show ipv6 ospf route

Output
Figure 22-16: Example output from the show ipv6 ospf P10 route command for a specific process

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;process-id&gt;</td>
<td>A character string that specifies the router process. If this parameter is included, only the information for this specified routing process is displayed.</td>
</tr>
</tbody>
</table>

OSPFv3 Process (P1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area

<table>
<thead>
<tr>
<th>E1 - OSPF external type 1, E2 - OSPF external type 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>O 2002:1111::/64</td>
</tr>
<tr>
<td>via fe80::200:cdff:fe24:daae, vlan3, Area 0.0.0.0</td>
</tr>
<tr>
<td>C 2003:1111::/64</td>
</tr>
<tr>
<td>directly connected, vlan3, Area 0.0.0.0</td>
</tr>
<tr>
<td>O 2004:1111::/64</td>
</tr>
<tr>
<td>via fe80::200:cdff:fe24:daae, vlan3, Area 0.0.0.0</td>
</tr>
<tr>
<td>C 2005:1111::/64</td>
</tr>
<tr>
<td>directly connected, vlan5, Area 0.0.0.0</td>
</tr>
<tr>
<td>E2 2010:2222::/64</td>
</tr>
<tr>
<td>via 2003:1111::1, vlan3</td>
</tr>
<tr>
<td>E2 2011:2222::/64</td>
</tr>
<tr>
<td>via 2003:1111::1, vlan3</td>
</tr>
<tr>
<td>E2 2012:2222::/64</td>
</tr>
<tr>
<td>via 2003:1111::1, vlan3</td>
</tr>
<tr>
<td>E2 2013:2222::/64</td>
</tr>
<tr>
<td>via 2003:1111::1, vlan3</td>
</tr>
<tr>
<td>E2 2014:2222::/64</td>
</tr>
<tr>
<td>via 2003:1111::1, vlan3</td>
</tr>
<tr>
<td>E2 2015:2222::/64</td>
</tr>
<tr>
<td>via 2003:1111::1, vlan3</td>
</tr>
</tbody>
</table>

OSPFv3 for IPv6 Commands
Show IPv6 OSPF Route
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show ipv6 ospf virtual-links

**Mode**  
User Exec and Privileged Exec

**Usage**  
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 22-17: 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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipv6-addr/prefix-length&gt;</td>
<td>Specifies the base IPv6 address of the IPv6 summary address. The range of addresses given as IPv6 starting address and an IPv6 prefix length.</td>
</tr>
<tr>
<td>not-advertise</td>
<td>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.</td>
</tr>
<tr>
<td>tag &lt;0-4294967295&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 \texttt{summary-address} command to aggregate external LSAs that match the IPv6 prefix \texttt{2001:0db8::/32} and assigns a tag value of \texttt{3}.

\begin{verbatim}
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# summary-address 2001:0db8::/32 tag 3
\end{verbatim}

The following example uses the \texttt{no summary-address} command to stop summarizing IPv6 addresses in the address range covered within the IPv6 prefix \texttt{2001:0db8::/32}.

\begin{verbatim}
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no summary-address 2001:0db8::/32
\end{verbatim}
timers spf (IPv6 OSPF) (deprecated)

**Overview**  Use this command to adjust route calculation timers.

Use the `no` variant of this command to return to the default timer values.

**Syntax**
```
timers spf <spf-delay> <spf-holdtime>
no timers spf
```

**Default**  The default `spf-delay` value is 5 seconds. The default `spf-holdtime` value is 10 seconds.

**Mode**  Router Configuration

**Usage**  This command configures the delay time between the receipt of a topology change and the calculation of the Shortest Path First (SPF). This command also configures the hold time between two consecutive SPF calculations.

**Examples**
```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# timers spf 7 12
```

**Related Commands**
- timers spf exp (IPv6 OSPF)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `<spf-delay>` | `<0-2147483647>`  
Specifies the delay between receiving changed routing information and embarking on an SPF calculation. |
| `<spf-holdtime>` | `<0-2147483647>`  
Specifies the hold time between consecutive SPF calculations. |
**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>
```

**Mode** Router Configuration

**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 ipv6 ospf 100
awplus(config-router)# timers spf exp 5 20
```

**Related Commands** timers spf (IPv6 OSPF) (deprecated)
**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.
**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.
Overview

This command applies the functionality of the no debug ipv6 ospf packet command.
**Overview** This command applies the functionality of the **no debug ipv6 ospf route** command.
Introduction

Overview  This chapter provides an alphabetical reference for route map commands. These commands can be divided into the following categories:

- **route-map** command, 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 the route map applies to
- **set** commands, used to modify matching routes

Command List  

- “match interface” on page 1022
- “match ip address” on page 1023
- “match ip next-hop” on page 1025
- “match ipv6 address” on page 1027
- “match metric” on page 1028
- “match route-type” on page 1029
- “match tag” on page 1030
- “route-map” on page 1031
- “set ip next-hop (route map)” on page 1033
- “set metric” on page 1034
- “set metric-type” on page 1036
- “set tag” on page 1037
- “show route-map” on page 1038
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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>The VLAN to match, e.g. vlan2.</td>
</tr>
</tbody>
</table>

**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
ROUTE MAP COMMANDS

MATCH IP ADDRESS

**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.

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 route map action and its **set** clauses determine what the route map does with routes that contain that prefix.

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 {<accesslistID>|prefix-list <prefix-listname>}
no match ip address [<accesslistID>]
no match ip address prefix-list <prefix-listname>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;accesslistID&gt;</code></td>
<td>`{&lt;access-list-name&gt;</td>
</tr>
<tr>
<td><code>&lt;access-list-name&gt;</code></td>
<td>The IP access list name.</td>
</tr>
<tr>
<td><code>&lt;1-199&gt;</code></td>
<td>The IP access list number.</td>
</tr>
<tr>
<td><code>&lt;1300-2699&gt;</code></td>
<td>The IP access list number (expanded range).</td>
</tr>
<tr>
<td><strong>prefix-list</strong></td>
<td>Use an IP prefix list to specify which prefixes to match.</td>
</tr>
<tr>
<td><code>&lt;prefix-listname&gt;</code></td>
<td>The prefix list name.</td>
</tr>
</tbody>
</table>

**Mode** Route-map Configuration

**Usage** The **match ip address** command specifies the IP address to be matched. If there is a match for the specified IP 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 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
- 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:

```bash
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:

```bash
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 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 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 {<accesslistID>|prefix-list <prefix-listname>}
no match ip next-hop [<accesslistID>]
no match ip next-hop prefix-list [<prefix-listname>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;accesslistID&gt;</code></td>
<td>`&lt;access-list-name&gt;</td>
</tr>
<tr>
<td><code>&lt;access-list-name&gt;</code></td>
<td>The IP access list name.</td>
</tr>
<tr>
<td><code>&lt;1-199&gt;</code></td>
<td>The IP access list number.</td>
</tr>
<tr>
<td><code>&lt;1300-2699&gt;</code></td>
<td>The IP access list number (expanded range).</td>
</tr>
<tr>
<td><code>prefix-list</code></td>
<td>Use an IP prefix list to specify which next hop to match.</td>
</tr>
<tr>
<td><code>&lt;prefix-listname&gt;</code></td>
<td>The prefix list name.</td>
</tr>
</tbody>
</table>

**Mode** Route-map Configuration
ROUTE MAP COMMANDS
MATCH IP NEXT-HOP

Usage
This command is valid for:

- OSPF routes
- 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
```
ROUTE MAP COMMANDS

MATCH IPV6 ADDRESS

match ipv6 address

Overview
Use this command to specify the match address of route.

Use the no variant of this command to remove the match ipv6 address entry.

Syntax
match ipv6 address {
<access-list-name>
| prefix-list

no match ipv6 address [<access-list-name>|prefix-list

Mode
Route-map Configuration

Usage
The match ipv6 address <access-list> command specifies the IPv6 address to be matched. If there is a match for the specified IPv6 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.

The match ipv6 address prefix-list command specifies the entries of prefix-lists to be matched. If there is a match for the specified prefix-list entries, 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.

Examples
awplus# configure terminal
awplus(config)# route-map rmap1 deny 1
awplus(config-route-map)# match ipv6 address rmap1
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# match ipv6 address prefix-list mylist

Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;access-list-name&gt;</td>
<td>The name of the IPv6 access list that specifies criteria for the addresses to match. Valid only with RIPng.</td>
</tr>
<tr>
<td>&lt;prefix-listname&gt;</td>
<td>The name of the IPv6 prefix list that specifies criteria for the addresses to be matched. Valid only with RIPng.</td>
</tr>
</tbody>
</table>
**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.

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**
```
<metric>
```

**Description**
```
<0-4294967295> Specifies the metric value.
```

**Mode**
Route-map Configuration

**Usage**
This command is valid for:

- OSPF routes
- 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 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**
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type-1</td>
</tr>
<tr>
<td>type-2</td>
</tr>
</tbody>
</table>

**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.

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 match the entry.
- one or more of the set commands to create set clauses. These change the attributes of matching routes.

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>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mapname&gt;</td>
<td>A name to identify the route map.</td>
</tr>
<tr>
<td>deny</td>
<td>The route map causes a routing process to discard matching routes.</td>
</tr>
<tr>
<td>permit</td>
<td>The route map causes a routing process to use matching routes.</td>
</tr>
<tr>
<td>&lt;seq&gt;</td>
<td>The sequence number of the entry. You can use this parameter to control the order of entries in this route map.</td>
</tr>
</tbody>
</table>

Mode
Global Configuration

Usage
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:

- redistributes routes from one routing protocol into another
- redistributes static routes into routing protocols

When a routing protocol passes a route 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.
ROUTE MAP COMMANDS

ROUTE-MAP

If it does not find a match, it discards the route. This means that route maps end with an implicit deny entry. To permit all non-matching routes, 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 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 OSPF:

- `distribute-list (OSPF)`
- `default-information originate (OSPF)`
- `redistribute (OSPF)`

For RIP:

- `redistribute (RIP)`
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 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>]
```

**Mode**
Route-map Configuration

**Usage**
Use this command to set the next-hop IP address to the routes.
This command is valid for:
- OSPF routes
- 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 metric**

**Overview**  Use this command to add a metric set clause to a route map entry.

When a route matches the route map entry, the device takes one of the following actions:

- changes the metric to the specified value, or
- adds or subtracts the specified value from the metric, 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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Increase the metric by the specified amount.</td>
</tr>
<tr>
<td>-</td>
<td>Decrease the metric by the specified amount.</td>
</tr>
<tr>
<td>&lt;metric-value&gt;</td>
<td>&lt;0-4294967295&gt;</td>
</tr>
<tr>
<td></td>
<td>The new metric value, or the amount by which to increase or decrease the existing value.</td>
</tr>
</tbody>
</table>

**Default**  The default metric value for routes redistributed into OSPF and OSPFv3 is 20.

**Mode**  Route-map Configuration

**Usage**  This command is valid for:

- OSPF routes
- 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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type-1</td>
<td>Redistribute matching routes into OSPF as type-1 external routes.</td>
</tr>
<tr>
<td>type-2</td>
<td>Redistribute matching routes into OSPF as type-2 external routes.</td>
</tr>
</tbody>
</table>

**Mode**  
Route-map Configuration

**Usage**  
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 (OSPF)  
redistribute (OSPF)  
match route-type  
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;tag-value&gt;</td>
<td>&lt;0-4294967295&gt;</td>
</tr>
<tr>
<td></td>
<td>Value to tag matching routes with.</td>
</tr>
</tbody>
</table>

**Mode**
Route-map Configuration

**Usage**
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 (OSPF)
- redistribute (OSPF)
- match tag
- 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>
```

**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 23-1:  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
Introduction

Overview

This chapter provides an alphabetical reference of generic multicast commands. For commands for particular 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. 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.
MULTICAST COMMANDS

Command List

- "clear ip mroute" on page 1041
- "clear ip mroute statistics" on page 1042
- "clear ipv6 mroute" on page 1043
- "clear ipv6 mroute statistics" on page 1044
- "debug nsm mcast" on page 1045
- "debug nsm mcast6" on page 1046
- "ip mroute" on page 1047
- "ip multicast forward-first-packet" on page 1049
- "ip multicast route" on page 1050
- "ip multicast route-limit" on page 1052
- "ip multicast wrong-vif-suppression" on page 1053
- "ip multicast-rout"ing on page 1054
- "ipv6 multicast route" on page 1055
- "ipv6 multicast route-limit" on page 1058
- "ipv6 multicast-rout"ing on page 1059
- "multicast" on page 1060
- "show ip mroute" on page 1061
- "show ip mvif" on page 1063
- "show ip rpf" on page 1064
- "show ipv6 mroute" on page 1065
- "show ipv6 mvif" on page 1067
**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]
```

**Mode**  
Privileged Exec

**Usage**  
When this command is used, the Multicast Routing Information Base (MRIB) clears the IPv4 multicast route entries in its IPv4 multicast route table, and removes the entries from the multicast forwarder. The MRIB sends a “clear” message to the multicast protocols. Each multicast protocol has its own “clear” multicast route command. The protocol-specific “clear” command clears multicast routes from PIM Sparse Mode, and also clears the routes from the MRIB.

**Examples**  
```
awplus# clear ip mroute 225.1.1.1 192.168.3.3
awplus# clear ip mroute *
```

**Related Commands**  
- ip multicast route
- show ip mroute
clear ip mroute statistics

**Overview**  Use this command to delete multicast route statistics entries from the IP multicast routing table.

**Syntax**  
```
clear ip mroute statistics {*-<ipv4-group-addr> [<-ipv4-source-addr>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>All multicast route entries.</td>
</tr>
<tr>
<td>&lt;ipv4-group-addr&gt;</td>
<td>Group IPv4 address, in dotted decimal notation in the format A.B.C.D.</td>
</tr>
<tr>
<td>&lt;ipv4-source-addr&gt;</td>
<td>Source IPv4 address, in dotted decimal notation in the format A.B.C.D.</td>
</tr>
</tbody>
</table>

**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>]]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Deletes all dynamically-learned IPv6 multicast routes.</td>
</tr>
<tr>
<td><code>&lt;ipv6-group-address&gt;</code></td>
<td>Group IPv6 address, in hexadecimal notation in the format X.X::X.X.</td>
</tr>
<tr>
<td><code>&lt;ipv6-source-address&gt;</code></td>
<td>Source IPv6 address, in hexadecimal notation in the format X.X::X.X.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Usage**  When this command is used, the Multicast Routing Information Base (MRIB) clears the relevant IPv6 multicast route entries in its IPv6 multicast route table, and removes the entries from the multicast forwarder. The MRIB sends a “clear” message to the multicast protocols. Each multicast protocol has its own “clear” multicast route command.

This command does not remove static routes from the routing table or the configuration. To remove static routes, use the no parameter of the command `ipv6 multicast route`.

**Example**  
```
awplus# clear ipv6 mroute 2001::2 ff08::1
```

**Related Commands**  
- `ipv6 multicast route`
- `show ipv6 mroute`
clear ipv6 mroute statistics

**Overview**  Use this command to delete multicast route statistics entries from the IPv6 multicast routing table.

*NOTE:* Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the `clear ipv6 mroute` command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous static IPv6 multicast routes.

**Syntax**

```
clear ipv6 mroute statistics {*|<ipv6-group-address> [<ipv6-source-address>]} 
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>All multicast route entries.</td>
</tr>
<tr>
<td><code>&lt;ipv6-group-addr&gt;</code></td>
<td>Group IPv6 address, in hexadecimal notation in the format X.X::X.X.</td>
</tr>
<tr>
<td><code>&lt;ipv6-source-addr&gt;</code></td>
<td>Source IPv6 address, in hexadecimal notation in the format X.X::X.X.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Examples**

```
awplus# clear ipv6 mroute statistics 2001::2 ff08::1
awplus# clear ipv6 mroute statistics *
```
**debug nsm mcast**

**Overview**  Use this command to debug IPv4 events in the Multicast Routing Information Base (MRIB).

**Syntax**

```
debug nsm mcast
{all|fib-msg|mrt|mtrace|mtrace-detail|register|stats|vif}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All IPv4 multicast debugging.</td>
</tr>
<tr>
<td>fib-msg</td>
<td>Forwarding Information Base (FIB) messages.</td>
</tr>
<tr>
<td>mrt</td>
<td>Multicast routes.</td>
</tr>
<tr>
<td>mtrace</td>
<td>Multicast traceroute.</td>
</tr>
<tr>
<td>mtrace-detail</td>
<td>Multicast traceroute detailed debugging.</td>
</tr>
<tr>
<td>register</td>
<td>Multicast PIM register messages.</td>
</tr>
<tr>
<td>stats</td>
<td>Multicast statistics.</td>
</tr>
<tr>
<td>vif</td>
<td>Multicast interface.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec and Global Configuration

**Examples**

```
awplus# configure terminal
awplus(config)# debug nsm mcast all
awplus# configure terminal
awplus(config)# debug nsm mcast fib-msg
awplus# configure terminal
awplus(config)# debug nsm mcast mrt
awplus# configure terminal
awplus(config)# debug nsm mcast mtrace
awplus# configure terminal
awplus(config)# debug nsm mcast mtrace-detail
awplus# configure terminal
awplus(config)# debug nsm mcast register
awplus# configure terminal
awplus(config)# debug nsm mcast stat
awplus# configure terminal
awplus(config)# debug nsm mcast vif
```
**debug nsm mcast6**

**Overview**
Use this command to debug IPv6 events in the Multicast Routing Information Base (MRIB).

**Syntax**
```
default nsm mcast6
   {all|fib-msg|mrt|mtrace|mtrace-detail|register|stats|vif}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All IPv4 multicast debugging.</td>
</tr>
<tr>
<td>fib-msg</td>
<td>Forwarding Information Base (FIB) messages.</td>
</tr>
<tr>
<td>mif</td>
<td>Multicast interfaces.</td>
</tr>
<tr>
<td>mrt</td>
<td>Multicast routes.</td>
</tr>
<tr>
<td>register</td>
<td>Multicast PIM register messages.</td>
</tr>
<tr>
<td>stats</td>
<td>Multicast statistics.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec and Global Configuration

**Examples**
```
awplus# configure terminal
awplus(config)# debug nsm mcast6 all
awplus# configure terminal
awplus(config)# debug nsm mcast6 fib-msg
awplus# configure terminal
awplus(config)# debug nsm mcast6 mif
awplus# configure terminal
awplus(config)# debug nsm mcast6 mrt
awplus# configure terminal
awplus(config)# debug nsm mcast6 register
awplus# configure terminal
awplus(config)# debug nsm mcast6 stats
```
**ip mroute**

**Overview**
Use this command to inform multicast of the RPF (Reverse Path Forwarding) route to a given IPv4 multicast source.

Use the **no** variant of this command to delete a route to an IPv4 multicast source.

**Syntax**
```
ip mroute <ipv4-source-address/mask-length> [bgp|ospf|rip|static] <rpf-address> [<admin-distance>]
no ip mroute <ipv4-source-address/mask-length> [bgp|ospf|rip|static]
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipv4-source-address/mask-length&gt;</td>
<td>A multicast source IPv4 address and mask length, in dotted decimal notation in the format A.B.C.D/M.</td>
</tr>
<tr>
<td>ospf</td>
<td>OSPF unicast routing protocol.</td>
</tr>
<tr>
<td>rip</td>
<td>RIP unicast routing protocol.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies a static route.</td>
</tr>
<tr>
<td>&lt;rpf-address&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;admin-distance&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Usage**
Typically, when a Layer 3 multicast routing protocol is determining the RPF (Reverse Path Forwarding) interface for the path to an IPv4 multicast source, it uses the unicast route table to find the best path to the source. However, in some networks a deliberate choice is made to send multicast via different paths to those used for unicast. In this case, the interface via which a multicast stream from a given source enters a router may not be the same as the interface that connects to the best unicast route to that source.

This command enables the user to statically configure the device with “multicast routes” back to given sources. When performing the RPF check on a stream from a given IPv4 source, the multicast routing protocol will look at these static entries as well as looking into the unicast routing table. The route with the lowest administrative distance - whether a static “multicast route” or a route from the unicast route table - will be chosen as the RPF route to the source.
Note that in this context the term “multicast route” does not imply a route via which the current router will forward multicast; instead it refers to the route the multicast will have traversed in order to arrive at the current router.

**Examples**

The following example creates a static multicast IPv4 route back to the sources in the 10.10.3.0/24 subnet. The multicast route is via the host 192.168.2.3, and has an administrative distance of 2:

```
awplus# configure terminal
awplus(config)# ip mroute 10.10.3.0/24 static 2 192.168.2.3 2
```

The following example creates a static multicast IPv4 route back to the sources in the 192.168.3.0/24 subnet. The multicast route is via the host 10.10.10.50. The administrative distance on this route has the default value of 0:

```
awplus# configure terminal
awplus(config)# ip mroute 192.168.3.0/24 10.10.10.50
```

**Validation Commands**

`show ip rpf`
ip multicast forward-first-packet

**Overview**  
Use this command to enable multicast to forward the first multicast packets coming to the device.

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

**Syntax**  
```
ip multicast forward-first-packet
no ip multicast forward-first-packet
```

**Default**  
By default, this feature is disabled.

**Mode**  
Global Configuration

**Usage**  
If this command is enabled, the device will forward the first packets in a multicast stream that create the multicast route, possibly causing degradation in the quality of the multicast stream, such as the pixelation of video and audio data.

*NOTE: If you use this command, ensure that the ip igmp snooping command is enabled, the default setting, otherwise the device will not process the first packets of the multicast stream correctly.*

The device will forward the first multicast packets to all interfaces which are on the same VLAN as those which asked for this multicast group.

**Examples**  
To enable the forwarding of the first multicast packets, use the following commands:
```
awplus# configure terminal
awplus(config)# ip multicast forward-first-packet
```

To disable the forwarding of the first multicast packets, use the following commands:
```
awplus# configure terminal
awplus(config)# no ip multicast forward-first-packet
```
ip multicast route

**Overview** Use this command to add an IPv4 static multicast route for a specific multicast source and group IPv4 address to the multicast Routing Information Base (RIB). This IPv4 multicast route is used to forward multicast traffic from a specific source and group ingressing on an upstream VLAN to a single or range of downstream VLANs.

Use the `no` variant of this command to either remove an IPv4 static multicast route set with this command or to remove a specific downstream VLAN interface from an IPv4 static multicast route for a specific multicast source and group IPv4 address.

**Syntax**
```
ip multicast route <ipv4-source-addr> <ipv4-group-addr> <upstream-vlan-id> [ <downstream-vlan-id> ]
no ip multicast route <ipv4-source-addr> <ipv4-group-addr> [ <upstream-vlan-id> <downstream-vlan-id> ]
```

**Default** By default, this feature is disabled.

**Mode** Global Configuration

**Usage** Only one multicast route entry per IPv4 address and multicast group can be specified. Therefore, if one entry for a static multicast route is configured, PIM will not be able to update this multicast route in any way.

If a dynamic multicast route exists you cannot create a static multicast route with same source IPv4 address, group IPv4 address, upstream VLAN and downstream VLANs. An error message is displayed and logged. To add a new static multicast route, either wait for the dynamic multicast route to timeout or clear the dynamic multicast route with the `clear ip mroute` command.

To update an existing static multicast route entry with more or a new set of downstream VLANs, you must firstly remove the existing static multicast route and then add the new static multicast route with all downstream VLANs specified. If you attempt to update an existing static multicast route entry with an additional VLAN or VLANs an error message is displayed and logged.

To create a blackhole or null route where packets from a specified source and group address coming from an upstream VLAN are dropped rather than...
MULTICAST COMMANDS
IP MULTICAST ROUTE

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 IPv4 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]
nop multicast route-limit
```

**Default**  The default limit and threshold value is 2147483647.

**Mode**  Global Configuration

**Usage**  This command limits the number of multicast IPv4 routes (mroutes) that can be added to a router, and generates an error message when the limit is exceeded. If the threshold parameter is set, a threshold warning message is generated when this threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the limit argument.

**Examples**  
```
awplus# configure terminal
awplus(config)# ip multicast route-limit 34 24
awplus# configure terminal
awplus(config)# no ip multicast route-limit
```
ip multicast wrong-vif-suppression

**Overview**  Use this command to prevent unwanted multicast packets received on an unexpected VLAN being trapped to the CPU. Use the no variant of this command to disable wrong VIF suppression.

**Syntax**  
```
ip multicast wrong-vif-suppression
no ip multicast wrong-vif-suppression
```

**Default**  By default, this feature is disabled.

**Mode**  Global Configuration

**Usage**  Use this command if there is excessive CPU load and multicast traffic is enabled. To confirm that VIF messages are being sent to the CPU use the `debug nsm mcast6` command.

**Examples**  To enable the suppression of wrong VIF packets, use the following commands:
```
awplus# configure terminal
awplus(config)# ip multicast wrong-vif-suppression
```
To disable the suppression of wrong VIF packets, use the following commands:
```
awplus# configure terminal
awplus(config)# no ip multicast wrong-vif-suppression
```
Multicast Commands
IP Multicast-Routing

ip multicast-routing

**Overview**
Use this command to turn on/off IPv4 multicast routing on the router; when turned off the device does not perform multicast functions.

Use the `no` variant of this command to disable IPv4 multicast routing after enabling it. Note the default stated below.

**Syntax**
```
ip multicast-routing
no ip multicast-routing
```

**Default**
By default, IPv4 multicast routing is off.

**Mode**
Global Configuration

**Usage**
When the `no` variant of this command is used, the Multicast Routing Information Base (MRIB) cleans up Multicast Routing Tables (MRT), stops IGMP operation, and stops relaying multicast forwarder events to multicast protocols.

When multicast routing is enabled, the MRIB starts processing any MRT addition/deletion requests, and any multicast forwarding events.

You must enable multicast routing before issuing other multicast commands.

**Example**
```
awplus# configure terminal
awplus(config)# ip multicast-routing
```

**Validation Commands**
`show running-config`
**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> ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv6-source-addr&gt;</code></td>
<td>Source IPv6 address, in dotted decimal notation in the format X.X::X.X.</td>
</tr>
<tr>
<td><code>&lt;ipv6-group-addr&gt;</code></td>
<td>Group IP address, in dotted decimal notation in the format X.X::X.X.</td>
</tr>
<tr>
<td><code>&lt;upstream-vlan-id&gt;</code></td>
<td>Upstream VLAN interface on which the multicast packets ingress.</td>
</tr>
<tr>
<td><code>&lt;downstream-vlan-id&gt;</code></td>
<td>Downstream VLAN interface or range of VLAN interfaces to which the multicast packets are sent.</td>
</tr>
</tbody>
</table>

**Default**

By default, no static routes exist.

**Mode**

Global Configuration

**Usage**

Only one multicast route entry per IPv6 address and multicast group can be specified. Therefore, if one entry for an IPv6 static multicast route is configured, PIM will not be able to update this multicast route in any way.

If a dynamic multicast route exists, you cannot create a static multicast route with the same source IPv6 address and group IPv6 address. An error message is displayed and logged. To add a new static multicast route, either wait for the dynamic multicast route to time out or clear the dynamic multicast route with the `clear ipv6 mroute` command.

To update an existing IPv6 static multicast route entry with new or additional downstream VLANs, you must firstly remove the existing static multicast route and then add the new static multicast route with all downstream VLANs specified. If
you attempt to update an existing static multicast route entry with an additional VLAN or VLANs an error message is displayed and logged.

To 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:

**Output**  Figure 24-1: 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**  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
```
**Overview**
Use this command to turn on/off IPv6 multicast routing on the router; when turned off the device does not perform multicast functions.

Use the **no** variant of this command to disable IPv6 multicast routing after enabling it. Note the default stated below.

**Syntax**

```
ipv6 multicast-routing
no ipv6 multicast-routing
```

**Default**
By default, IPv6 multicast routing is off.

**Mode**
Global Configuration

**Usage**

When the **no** variant of this command is used, the Multicast Routing Information Base (MRIB) cleans up Multicast Routing Tables (MRT, and stops relaying multicast forwarder events to multicast protocols.

When multicast routing is enabled, the MRIB starts processing any MRT addition/deletion requests, and any multicast forwarding events.

You must enable multicast routing before issuing other multicast commands.

**Examples**

```
awplus# configure terminal
awplus(config)# ipv6 multicast-routing
awplus# configure terminal
awplus(config)# no ipv6 multicast-routing
```

**Validation Commands**

```
show running-config
```
**multicast**

**Overview**  Use this command to enable a device port to route multicast packets that ingress the port.

Use the no variant of this command to stop the device port from routing multicast packets that ingress the port. Note that this does not affect Layer 2 forwarding of multicast packets. If you enter no multicast on a port, multicast packets received on that port will not be forwarded to other VLANs, but ports in the same VLANs as the receiving port will still receive the multicast packets.

**Syntax**  
- multicast
- no multicast

**Default**  By default, all device ports route multicast packets.

**Mode**  Interface Configuration

**Examples**  
```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# multicast
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no multicast
```

**Validation Commands**  show running-config
show ip mroute

**Overview**  Use this command to display the contents of the IPv4 multicast routing (mroute) table.

**Syntax**  
```
show ip mroute [<ipv4-group-addr>] [<ipv4-source-addr>] [{dense|sparse}] [{count|summary}]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv4-group-addr&gt;</code></td>
<td>Group IPv4 address, in dotted decimal notation in the format A.B.C.D.</td>
</tr>
<tr>
<td><code>&lt;ipv4-source-addr&gt;</code></td>
<td>Source IPv4 address, in dotted decimal notation in the format A.B.C.D.</td>
</tr>
<tr>
<td>dense</td>
<td>Display dense IPv4 multicast routes.</td>
</tr>
<tr>
<td>sparse</td>
<td>Display sparse IPv4 multicast routes.</td>
</tr>
<tr>
<td>count</td>
<td>Display the route and packet count from the IPv4 multicast routing (mroute) table.</td>
</tr>
<tr>
<td>summary</td>
<td>Display the contents of the IPv4 multicast routing (mroute) table in an abbreviated form.</td>
</tr>
</tbody>
</table>

**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:

```
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)
```
### MULTICAST COMMANDS

#### SHOW IP MROUTE

**Figure 24-3:** Example output from the `show ip mroute` command with the source and group IPv4 address specified

```
awplus# show ip mroute 10.10.1.52 224.0.1.3
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), uptime 00:03:24, stat expires 00:01:28
Owner PIM-SM, Flags: TF
  Incoming interface: 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 24-4:** Example output from the `show ip mroute count` command

```
awplus# show ip mroute count
IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0/0
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 24-5:** Example output from the `show ip mroute summary` command

```
awplus# show ip mroute summary
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM, Flags: TF
```
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>The interface to display information about.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**  `awplus# show ip mvif vlan2`

**Output**  Figure 24-6: Example output from the `show ip mvif` command

```
Figure 24-7: Example output from the `show ip mvif` command with the `vlan2` specified
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vif</th>
<th>Owner</th>
<th>TTL</th>
<th>Local</th>
<th>Remote</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Idx</td>
<td>Module</td>
<td></td>
<td>Address</td>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>vlan2</td>
<td>0</td>
<td>PIM-SM</td>
<td>1</td>
<td>192.168.1.53</td>
<td>0.0.0.0</td>
<td>00:04:26</td>
</tr>
<tr>
<td>Register</td>
<td>1</td>
<td></td>
<td>1</td>
<td>192.168.1.53</td>
<td>0.0.0.0</td>
<td>00:04:26</td>
</tr>
<tr>
<td>vlan3</td>
<td>2</td>
<td>PIM-SM</td>
<td>1</td>
<td>192.168.10.53</td>
<td>0.0.0.0</td>
<td>00:04:25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vif</th>
<th>Owner</th>
<th>TTL</th>
<th>Local</th>
<th>Remote</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Idx</td>
<td>Module</td>
<td></td>
<td>Address</td>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>vlan2</td>
<td>0</td>
<td>PIM-SM</td>
<td>1</td>
<td>192.168.1.53</td>
<td>0.0.0.0</td>
<td>00:05:17</td>
</tr>
</tbody>
</table>
**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>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv4-source-addr&gt;</code></td>
<td>Source IPv4 address, in dotted decimal notation in the format A.B.C.D.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Example**  
`awplus# show ip rpf 10.10.10.50`
**show ipv6 mroute**

**Overview**  
Use this command to display the contents of the IPv6 multicast routing (mroute) table.

**Syntax**
```
show ipv6 mroute [<ipv6-group-addr>] [<ipv6-source-addr>] [{count|summary}]
```

**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
```

**Parameter**
- **<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.

**Output**  
The following is a sample output of this command displaying the IPv6 multicast routing table for a single static IPv6 Multicast route:

```
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:
MULTICAST COMMANDS
SHOW IPV6 MROUTE

Figure 24-9: 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 24-10: Example output from the show ipv6 mroute summary command

awplus#show ipv6 mroute summary
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface

(2001::2, ff08::1), 03:20:28/-, IMI, Flags: F
show ipv6 mif

**Overview**  Use this command to display the contents of the IPv6 Multicast Routing Information Base (MRIB) MIF table.

**Syntax**  
show ipv6 mif [<interface>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>The interface to display information about.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**
awplus# show ipv6 mif
awplus# show ipv6 mif vlan2

**Output**  Figure 24-11: 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 24-12: 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
```
Introduction

Overview The Internet Group Management Protocol (IGMP) module includes the IGMP Proxy service and IGMP Snooping functionality. Some of the following commands may have commonalities and restrictions. These are described under the Usage section for each command.
IGMP AND IGMP SNOOPING COMMANDS

Command List

- “clear ip igmp” on page 1071
- “clear ip igmp group” on page 1072
- “clear ip igmp interface” on page 1073
- “debug igmp” on page 1074
- “ip igmp” on page 1075
- “ip igmp access-group” on page 1076
- “ip igmp immediate-leave” on page 1077
- “ip igmp last-member-query-count” on page 1078
- “ip igmp last-member-query-interval” on page 1079
- “ip igmp limit” on page 1080
- “ip igmp mroute-proxy” on page 1082
- “ip igmp proxy-service” on page 1083
- “ip igmp querier-timeout” on page 1084
- “ip igmp query-holdtime” on page 1085
- “ip igmp query-interval” on page 1087
- “ip igmp query-max-response-time” on page 1089
- “ip igmp ra-option (Router Alert)” on page 1091
- “ip igmp robustness-variable” on page 1092
- “ip igmp snooping” on page 1093
- “ip igmp snooping fast-leave” on page 1094
- “ip igmp snooping mrouter” on page 1095
- “ip igmp snooping querier” on page 1096
- “ip igmp snooping report-suppression” on page 1097
- “ip igmp snooping routernode” on page 1098
- “ip igmp snooping tcn query solicit” on page 1100
- “ip igmp source-address-check” on page 1102
- “ip igmp ssm” on page 1103
- “ip igmp ssm-map enable” on page 1104
- “ip igmp ssm-map static” on page 1105
- “ip igmp static-group” on page 1107
- “ip igmp startup-query-count” on page 1109
- “ip igmp startup-query-interval” on page 1110
- “ip igmp version” on page 1111
- “show debugging igmp” on page 1112
- “show ip igmp groups” on page 1113
• “show ip igmp interface” on page 1115
• “show ip igmp proxy” on page 1119
• “show ip igmp snooping mrouter” on page 1120
• “show ip igmp snooping routermode” on page 1121
• “show ip igmp snooping statistics” on page 1122
• “undebug igmp” on page 1123
clear ip igmp

**Overview**  Use this command to clear all IGMP group membership records on all VLAN interfaces.

**Syntax**  clear ip igmp

**Mode**  Privileged Exec

**Usage**  This command applies to VLAN interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

**Example**  awplus# clear ip igmp

**Validation Commands**

- show ip igmp interface
- show running-config

**Related Commands**

- clear ip igmp group
- clear ip igmp interface
clear ip igmp group

**Overview**  
Use this command to clear IGMP group membership records for a specific group on either all VLAN interfaces, a single VLAN interface, or for a range of VLAN interfaces.

**Syntax**  
clear ip igmp group *
clear ip igmp group <ip-address> <interface>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Clears all groups on all VLAN interfaces. This is an alias to the clear ip igmp command.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>Specifies the group whose membership records will be cleared from all VLAN interfaces, entered in the form A.B.C.D.</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>Specifies the name of the VLAN interface; all groups learned on this VLAN interface are deleted.</td>
</tr>
</tbody>
</table>

**Mode** Privileged Exec

**Usage**  
This command applies to groups learned by IGMP, IGMP Snooping, or IGMP Proxy. In addition to the group a VLAN interface can be specified. Specifying this will mean that only entries with the group learned on the interface will be deleted.

**Examples**  
awplus# clear ip igmp group *
awplus# clear ip igmp group 224.1.1.1 vlan1

**Validation Commands**  
show ip igmp interface
show running-config

**Related Commands**  
clear ip igmp
clear ip igmp interface
clear ip igmp interface

**Overview**  Use this command to clear IGMP group membership records on a particular VLAN interface.

**Syntax**  
`clear ip igmp interface <interface>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>Specifies the name of the VLAN interface. All groups learned on this VLAN interface are deleted.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Usage**  This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

**Example**  `awplus# clear ip igmp interface vlan1`

**Validation Commands**  
- `show ip igmp interface`
- `show running-config`

**Related Commands**  
- `clear ip igmp`
- `clear ip igmp group`
**debug igmp**

**Overview**
Use this command to enable debugging of either all IGMP or a specific component of IGMP.

Use the `no` variant of this command to disable all IGMP debugging, or debugging of a specific component of IGMP.

**Syntax**
```
debug igmp {all|decode|encode|events|fsm|tib}
no debug igmp {all|decode|encode|events|fsm|tib}
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enable or disable all debug options for IGMP</td>
</tr>
<tr>
<td>decode</td>
<td>Debug of IGMP packets that have been received</td>
</tr>
<tr>
<td>encode</td>
<td>Debug of IGMP packets that have been sent</td>
</tr>
<tr>
<td>events</td>
<td>Debug IGMP events</td>
</tr>
<tr>
<td>fsm</td>
<td>Debug IGMP Finite State Machine (FSM)</td>
</tr>
<tr>
<td>tib</td>
<td>Debug IGMP Tree Information Base (TIB)</td>
</tr>
</tbody>
</table>

**Modes**
Privileged Exec and Global Configuration

**Usage**
This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

**Example**
```
awplus# configure terminal
awplus(config)# debug igmp all
```

**Related Commands**
- `show debugging igmp`
- `undebug igmp`
**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**
This command can only be configured on VLAN interfaces, and will have no effect on IGMP Proxy or IGMP Snooping configuration.

*NOTE:*
An IP address must be assigned to the VLAN first, before this command will work.

**Example**
```
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;access-list-number&gt;</code></td>
<td>Standard IP access-list number, in the range <code>&lt;1-99&gt;</code>.</td>
</tr>
<tr>
<td><code>&lt;access-list-name&gt;</code></td>
<td>Standard IP access-list name.</td>
</tr>
</tbody>
</table>

**Default**
By default there are no access lists configured on any interface.

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
This command applies to VLAN interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

This command applies to VLAN interfaces configured for IGMP or IGMP Snooping.

**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 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**

```plaintext
ip igmp immediate-leave group-list
{<access-list-number>|<access-list-number-expanded>|<access-list-name>}
no ip igmp immediate-leave
```

**Default**  Disabled by default.

**Mode**  Interface Configuration for a VLAN interface.

**Usage**  This command applies to 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:

```plaintext
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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;access-list-number&gt;</code></td>
<td>Access-list number, in the range &lt;1-99&gt;.</td>
</tr>
<tr>
<td><code>&lt;access-list-number-expanded&gt;</code></td>
<td>Access-list number (expanded range), in the range &lt;1300-1999&gt;.</td>
</tr>
<tr>
<td><code>&lt;access-list-name&gt;</code></td>
<td>Standard IP access-list name.</td>
</tr>
</tbody>
</table>
**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**

```plaintext
ip igmp last-member-query-count <2-7>
no ip igmp last-member-query-count
```

**Default** The default last member query count value is 2.

**Mode** Interface Configuration for a VLAN interface.

**Usage** This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

**Example**

```plaintext
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp last-member-query-count 3
```

**Validation Commands**

- show ip igmp interface
- show running-config

**Related Commands**

- `ip igmp last-member-query-interval`
- `ip igmp startup-query-count`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;2-7&gt;</td>
<td>Last member query count value.</td>
</tr>
</tbody>
</table>
**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
```

**Default**

1000 milliseconds

**Mode**

Interface Configuration for a VLAN interface.

**Usage**

This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

**Example**

The following example changes the IGMP group-specific host query message interval to 2 seconds (2000 milliseconds) for VLAN interface vlan1:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip igmp last-member-query-interval 2000
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interval&gt;</td>
<td>The frequency in milliseconds, in the range &lt;1000-25500&gt;, at which IGMP group-specific host query messages are sent.</td>
</tr>
</tbody>
</table>

**Validation Commands**

- show ip igmp interface
- show running-config

**Related Commands**

- ip igmp immediate-leave
- ip igmp last-member-query-count
**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.

The limit is dependent on the MTU (Maximum Transmission Unit) of the interface, which is the size in bytes of the largest packet that a network protocol can transmit. Typically for an Ethernet channel with an MTU of 1500 the igmp group membership limit will be 183 groups, because each igmp group membership is 8 bytes.

Use the `no` variant of this command to unset the limit and any specified exception access-list.

**Syntax**

```plaintext
ip igmp limit <limitvalue> [except {<access-list-number>|<access-list-number-expanded>|<access-list-name>}]  
no ip igmp limit
```

**Parameter** | **Description**
--- | ---
<limitvalue> | <2-512> Maximum number of group membership entries.
<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**

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 `ip igmp limit` command.

The default limit of group membership entries that can be learned is 512 entries.

**Mode**

Global Configuration and Interface Configuration for a VLAN interface.

**Usage**

This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

**Examples**

The following example configures an IGMP limit of 100 group membership entries across all interfaces on which IGMP is enabled, and excludes group 224.1.1.1 from this limitation:

```
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
```
The following example configures an IGMP limit of 100 group membership entries on VLAN interface vlan2:

awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp limit 100
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 VLAN interface.

**Mode**  
Interface Configuration for a VLAN interface.

**Usage**  
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. This command applies to interfaces configured for IGMP Proxy.

**Example**  
The following example configures the VLAN interface `vlan2` as the upstream proxy-service interface for the downstream `vlan3` interface.  
```
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**  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.

**Example**  The following example designates the VLAN interface `vlan1` as the upstream proxy-service interface.

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip igmp proxy-service
```

**Related Commands**  `ip igmp mroute-proxy`
**ip igmp querier-timeout**

**Overview**
Use this command to configure the timeout period before the device takes over as the querier for the VLAN 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;timeout&gt;</code></td>
<td>IGMP querier timeout interval value in seconds, in the range <code>&lt;1-65535&gt;</code>.</td>
</tr>
</tbody>
</table>

**Default**
The default timeout interval is 255 seconds.

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
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**
The following example configures the device to wait 130 seconds from the time it received the last query before it takes over as the querier for the VLAN interface vlan20:
```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp querier-timeout 130
```

**Validation Commands**
- `show ip igmp interface`
- `show running-config`

**Related Commands**
- `ip igmp query-interval`
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interval&gt;</td>
<td>Query interval value in milliseconds, in the range &lt;100-5000&gt;.</td>
</tr>
</tbody>
</table>

**Default**  
By default the delay before sending IGMP General Query messages is 500 milliseconds.

**Mode**  
Interface Configuration for a VLAN interface.

**Usage**  
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.

**NOTE:**

*This command will function on your device in the stand-alone mode, but is not supported when the device forms part of a VCS Stack.*

**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:

```bash
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip igmp query-holdtime
```

**Validation Commands**

- `show ip igmp interface`
- `show running-config`

**Related Commands**

- `ip igmp query-interval`
- `ip igmp snooping tcn query solicit`
**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
```

**Default**
The default IGMP query interval is 125 seconds.

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
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**
The following example changes the period between IGMP host-query messages to 3 minutes (180 seconds) for VLAN interface vlan20:
```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp query-interval 180
```
IGMP AND IGMP SNOOPING COMMANDS

IP IGMP QUERY-INTERVAL

The following example resets the period between sending IGMP host-query messages to the default (125 seconds) for VLAN interface vlan20:

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# no ip igmp query-interval
```

**Validation Commands**

- show ip igmp interface
- show running-config

**Related Commands**

- ip igmp query-holdtime
- ip igmp query-max-response-time
- ip igmp startup-query-interval
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

Default
The default IGMP query maximum response time is 10 seconds.

Mode
Interface Configuration for a VLAN interface.

Usage
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
The following example configures a maximum response time of 8 seconds for VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp query-max-response-time 8
```

The following example restores the default maximum response time of 10 seconds for VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip igmp query-max-response-time
```
IGMP AND IGMP SNOOPING COMMANDS
IP IGMP QUERY-MAX-RESPONSE-TIME

**Validation Commands**
- show ip igmp interface
- show running-config

**Related Commands**
- ip igmp query-interval
**Overview**  Use this command to enable strict Router Alert (RA) option validation. With strict RA option enabled, IGMP packets without RA options are ignored.

**Syntax**

```plaintext
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**  This command applies to interfaces configured for IGMP and IGMP Snooping.

**Example**

```plaintext
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 a VLAN 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-7&gt;</td>
<td>The robustness variable value.</td>
</tr>
</tbody>
</table>

**Default**  The default robustness variable value is 2.

**Mode**  Interface Configuration for a VLAN interface.

**Usage**  This command applies to interfaces configured for IGMP and IGMP Snooping.

**Examples**
```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp robustness-variable 3
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# no ip igmp robustness-variable 3
```

**Validation Commands**
- `show ip igmp interface`
- `show running-config`
**Overview**  
Use this command to enable IGMP Snooping. When this command is used in the Global Configuration mode, IGMP Snooping is enabled at the device level. When this command is used in Interface Configuration mode, IGMP Snooping is enabled for the specified VLANs.

Use the **no** variant of this command to either globally disable IGMP Snooping, or disable IGMP Snooping on a specified interface.

**NOTE:** IGMP snooping cannot be disabled on an interface if IGMP snooping has already been disabled globally. IGMP snooping can be disabled on both an interface and globally if disabled on the interface first and then disabled globally.

**Syntax**
```
ip igmp snooping
no ip igmp snooping
```

**Default**  
By default, IGMP Snooping is enabled both globally and on all VLANs.

**Mode**  
Global Configuration and Interface Configuration for a VLAN interface.

**Usage**  
For IGMP snooping to operate on particular VLAN interfaces, it must be enabled both globally by using this command in Global Configuration mode, and on individual VLAN interfaces by using this command in Interface Configuration mode (both are enabled by default.)

Both IGMP snooping and MLD snooping must be enabled globally on the device for IGMP snooping to operate. MLD snooping is also enabled by default. To enable it if it has been disabled, use the `ipv6 mld snooping` command in Global Configuration mode.

**Examples**
```
awplus# configure terminal
awplus(config)# ip igmp snooping
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping
```

**Related Commands**
- `ipv6 mld snooping`
- `show ip igmp interface`
- `show running-config`
**ip igmp snooping fast-leave**

**Overview**
Use this command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing. The IGMP group-membership entry is removed as soon as an IGMP leave group message is received, without sending out a group-specific query.

Use the `no` variant of this command to disable fast-leave processing.

**Syntax**
```
ip igmp snooping fast-leave
no ip igmp snooping fast-leave
```

**Default**
IGMP Snooping fast-leave processing is disabled.

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
This IGMP Snooping command can only be configured on VLAN interfaces.

**Example**
This example shows how to enable fast-leave processing on the VLAN interface vlan2:
```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping fast-leave
```

**Validation Commands**
```
show ip igmp interface
show running-config
```
ip igmp snooping 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>
```

**Mode**  Interface Configuration for a VLAN interface.

**Example**  This example shows the switch port interface `port1.0.2` statically configured to be a multicast router interface for the VLAN interface `vlan2`:

```
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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;port&gt;</code></td>
<td>The port may be a device port (e.g. <code>port1.0.4</code>), a static channel group (e.g. <code>sa3</code>), or a dynamic (LACP) channel group (e.g. <code>po4</code>).</td>
</tr>
</tbody>
</table>
**ip igmp snooping querier**

**Overview**  Use this command to enable IGMP querier operation when no multicast routing protocol is configured. When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces. This command applies to interfaces configured for IGMP Snooping.

Use the `no` variant of this command to disable IGMP querier configuration.

**Syntax**  
```
ip igmp snooping querier
no ip igmp snooping querier
```

**Mode**  Interface Configuration for a VLAN interface.

**Usage**  
The IGMP Snooping querier uses the `0.0.0.0` Source IP address because it only masquerades as a proxy IGMP querier for faster network convergence.

It does not start, or automatically cease, the IGMP Querier operation if it detects query message(s) from a multicast router.

If an IP address is assigned to a VLAN, which has IGMP querier enabled on it, then the IGMP Snooping querier uses the VLAN’s IP address as the Source IP Address in IGMP queries.

The IGMP Snooping Querier will not stop sending IGMP Queries if there is another IGMP Snooping Querier in the network with a lower Source IP Address.

**NOTE:** Do not enable the IGMP Snooping Querier feature on a Layer 2 device when there is an operational IGMP Querier in the network.

**Example**  
```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping querier
```

**Validation Commands**
- `show ip igmp interface`
- `show running-config`
**ip igmp snooping report-suppression**

**Overview** Use this command to enable report suppression for IGMP versions 1 and 2. This command applies to interfaces configured for IGMP Snooping.

Report suppression stops reports being sent to an upstream multicast router port when there are already downstream ports for this group on this interface.

Use the `no` variant of this command to disable report suppression.

**Syntax**

```
ip igmp snooping report-suppression
no ip igmp snooping report-suppression
```

**Default** Report suppression does not apply to IGMPv3, and is turned on by default for IGMPv1 and IGMPv2 reports.

**Mode** Interface Configuration for a VLAN interface.

**Example** This example shows how to enable report suppression for IGMPv2 reports for the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp version 2
awplus(config-if)# ip igmp snooping report-suppression
```

**Validation Commands**

- `show ip igmp interface`
- `show running-config`
**Overview**

Use this command to set the destination IP addresses as a router multicast address, according to the routermode (all multicast addresses, default multicast addresses, specified multicast addresses).

Use the **no** variant of this command to the default. You can also remove a specified IP address from a custom list of multicast addresses.

**Syntax**

```plaintext
ip igmp snooping routermode
{all|default|ip|multicastrouter|address <ip-address>}
no ip igmp snooping routermode [address <ip-address>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All reserved multicast addresses (224.0.0.x). Packets from all possible addresses in range 224.0.0.x are set as routers.</td>
</tr>
<tr>
<td>default</td>
<td>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 set as routers.</td>
</tr>
<tr>
<td>ip</td>
<td>Custom reserved multicast addresses. Custom IP address in the 224.0.0.x range are set as router multicast addresses using the <code>ip igmp snooping routermode address &lt;ip-address&gt;</code> command.</td>
</tr>
<tr>
<td>multicastrouter</td>
<td>DVMRP (224.0.0.4) and PIM (224.0.0.13) multicast addresses are set as routers.</td>
</tr>
<tr>
<td>address</td>
<td>Specify the multicast address in the 224.0.0.x range for use after issuing an <code>ip igmp snooping routermode ip</code> command</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>IPv4 multicast address (224.0.0.x)</td>
</tr>
</tbody>
</table>

**Default**

The default routermode is **default** not **all** and shows the below reserved multicast addresses:
### IGMP AND IGMP SNOOPING COMMANDS

**IP IGMP SNOOPING ROUTERMODE**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Global Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples</td>
<td>To set <code>ip igmp snooping routermode</code> for all default reserved addresses enter:</td>
</tr>
<tr>
<td></td>
<td><code>awplus(config)# ip igmp snooping routermode default</code></td>
</tr>
<tr>
<td></td>
<td>To remove the multicast address 224.0.0.5 from the custom list of multicast addresses enter:</td>
</tr>
<tr>
<td></td>
<td><code>awplus(config)# no ip igmp snooping routermode address 224.0.0.5</code></td>
</tr>
<tr>
<td>Related commands</td>
<td><code>show ip igmp snooping routermode</code></td>
</tr>
</tbody>
</table>

**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
**ip igmp snooping tcn query solicit**

**Overview**

Use this command to enable IGMP (Internet Group Management Protocol) Snooping TCN (Topology Change Notification) Query Solicitation feature. When this command is used in the Global Configuration mode, Query Solicitation is enabled.

Use the `no` variant of this command to disable IGMP Snooping TCN Query Solicitation. When the `no` variant of this command is used in Interface Configuration mode, this overrides the Global Configuration mode setting and Query Solicitation is disabled.

**Syntax**

```
ip igmp snooping tcn query solicit
no ip igmp snooping tcn query solicit
```

**Default**

IGMP Snooping TCN Query Solicitation is disabled by default on the device, unless the device is the Master Node in an EPSR ring, or is the Root Bridge in a Spanning Tree.

When the device is the Master Node in an EPSR ring, or the device is the Root Bridge in a Spanning Tree, then IGMP Snooping TCN Query Solicitation is enabled by default and cannot be disabled using the Global Configuration mode command. However, Query Solicitation can be disabled for specified VLANs using this command from the Interface Configuration mode. Select the VLAN you want to disable in Interface Configuration mode then issue the `no` variant of this command to disable the specified VLAN without disabling this feature for other VLANs.

**Mode**

Global Configuration and Interface Configuration for a VLAN interface.

**Usage**

Once enabled, if the device is not an IGMP Querier, on detecting a topology change, the device generates IGMP Query Solicit messages that are sent to all the ports of the vlan configured for IGMP Snooping on the device.

On a device that is not the Master Node in an EPSR ring or the Root Bridge in a Spanning Tree, Query Solicitation can be disabled using the `no` variant of this command after being enabled.

If the device that detects a topology change is an IGMP Querier then the device will generate an IGMP Query message.

Note that the `no` variant of this command when issued in Global Configuration mode has no effect on a device that is the Master Node in an EPSR ring or on a device that is a Root Bridge in a Spanning Tree. Query Solicitation is not disabled for the device these instances. However, Query Solicitation can be disabled on a per-vlan basis from the Interface Configuration mode.

See the below state table that shows when Query Solicit messages are sent in these instances:
IGMP AND IGMP SNOOPING COMMANDS

IP IGMP SNOOPING TCN QUERY SOLICIT

<table>
<thead>
<tr>
<th>Command issued from Global Configuration</th>
<th>Device is STP Root Bridge or the EPSR Master Node</th>
<th>Command issued from Interface Configuration</th>
<th>IGMP Query Solicit message sent on VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

See the IGMP Feature Overview and Configuration Guide for introductory information about the Query Solicitation feature.

**NOTE:**

*This command will function on your device in the stand-alone mode, but is not supported when the device forms part of a VCS Stack.*

**Examples**

This example shows how to enable IGMP Snooping TCN Query Solicitation on a device:

```
awplus# configure terminal
awplus(config)# ip igmp snooping tcn query solicit
```

This example shows how to disable IGMP Snooping TCN Query Solicitation on a device:

```
awplus# configure terminal
awplus(config)# no ip igmp snooping tcn query solicit
```

This example shows how to enable IGMP Snooping TCN Query Solicitation for the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping tcn query solicit
```

This example shows how to disable IGMP Snooping TCN Query Solicitation for the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip igmp snooping tcn query solicit
```

**Validation Commands**

- show ip igmp interface
- show running-config

**Related Commands**

- ip igmp query-holdtime
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**  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 the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal  
awplus(config)# interface vlan2  
awplus(config-if)# ip igmp source-address-check
```

To allow IGMP Reports from outside the current subnet for the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal  
awplus(config)# interface vlan2  
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
```

**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**  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-expanded>|<access-list-name>} <ip-address>
oip igmp ssm-map static
{<access-list-number>|<access-list-number-expanded>|<access-list-name>} <ip-address>
```

**Parameter**  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;access-list-number&gt;</code></td>
<td>Access-list number, in the range &lt;1-99&gt;.</td>
</tr>
<tr>
<td><code>&lt;access-list-number-expanded&gt;</code></td>
<td>Access-list number (expanded range), in the range &lt;1300-1999&gt;.</td>
</tr>
<tr>
<td><code>&lt;access-list-name&gt;</code></td>
<td>Standard IP access-list name.</td>
</tr>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>Source address to use for static map group, entered in the form A.B.C.D.</td>
</tr>
</tbody>
</table>

**Mode**  
Global Configuration

**Usage**  
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>]
nop igmp static-group <ip-address> [source <ip-source-addr>|ssm-map] [interface <port>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>Standard IP Multicast group address, entered in the form A.B.C.D, to be configured as a static group member.</td>
</tr>
<tr>
<td>source</td>
<td>Optional.</td>
</tr>
<tr>
<td><code>&lt;ip-source-addr&gt;</code></td>
<td>Standard IP source address, entered in the form A.B.C.D, to be configured as a static source from where multicast packets originate.</td>
</tr>
<tr>
<td>ssm-map</td>
<td>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 <strong>ip igmp ssm-map static</strong> command.</td>
</tr>
<tr>
<td>interface</td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;port&gt;</code></td>
<td>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).</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration for a VLAN interface.
**Usage**  This command applies to IGMP operation on a specific interface to statically add group and/or source records, or to IGMP Snooping on a VLAN interface to statically add group and/or source records.

**Example**  The following example show how to statically add group and source records for IGMP on the VLAN interface vlan3:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip igmp
awplus(config-if)# ip igmp static-group 226.1.2.4 source 10.2.3.4
```
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;startup-query-count&gt;</td>
<td>Specify the IGMP startup query count for a VLAN interface in the range &lt;2-10&gt; where 2 is the default IGMP query count.</td>
</tr>
</tbody>
</table>

**Default**

The default IGMP startup query count is 2.

**Mode**

Interface Configuration for a VLAN interface.

**Examples**

The following example shows how to configure the IGMP startup query count to 4 for the VLAN interface `vlan3`:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip igmp startup-query-count 4
```

The following example shows how to remove the IGMP startup query count for the VLAN interface `vlan3`:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# no ip igmp startup-query-count
```

**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

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.

Examples
The following example shows how to configure the IGMP startup query interval to 15 seconds for the VLAN interface vlan2 to be one quarter of the IGMP query interval value of 60 seconds:

awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp startup-query-interval 15
awplus(config-if)# ip igmp query-interval 60

The following example shows how to remove the IGMP startup query interval for the VLAN interface vlan2:

awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip igmp startup-query-interval

Related Commands
ip igmp last-member-query-interval
ip igmp query-interval
ip igmp startup-query-count
ip igmp version

**Overview**  Use this command to set the current IGMP version (IGMP version 1, 2 or 3) on an interface.

Use the **no** variant of this command to return to the default version.

**Syntax**

(ip igmp version <1-3>)

no ip igmp version

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-3&gt;</td>
<td>IGMP protocol version number</td>
</tr>
</tbody>
</table>

**Default**  The default IGMP protocol version number is 3.

**Mode**  Interface Configuration for a VLAN interface.

**Usage**  This command applies to VLAN interfaces configured for IGMP.

**Example**

awplus# configure terminal
awplus(config)# interface vlan5
awplus(config-if)# ip igmp version 2

**Validation Commands**

show ip igmp interface
show debugging igmp

**Overview**  Use this command to display the IGMP debugging options set.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show debugging igmp

**Mode**  User Exec and Privileged Exec

**Example**  To display the IGMP debugging options set, enter the command:

```
awplus# show debugging igmp
```

**Output**  Figure 25-1:  Example output from the `show debugging igmp` command

```
IGMP Debugging status:
  IGMP Decoder debugging is on
  IGMP Encoder debugging is on
  IGMP Events debugging is on
  IGMP FSM debugging is on
  IGMP Tree-Info-Base (TIB) debugging is on
```

**Related Commands**  debug igmp
show ip igmp groups

**Overview**  Use this command to display the multicast groups with receivers directly connected to the router, and learned through IGMP.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show ip igmp groups [<ip-address>|<interface> detail]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>Address of the multicast group, entered in the form A.B.C.D.</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>Interface name for which to display local information.</td>
</tr>
</tbody>
</table>

**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 25-2:  Example output from the show ip igmp groups command

<table>
<thead>
<tr>
<th>IGMP Connected Group Membership</th>
<th>Group Address</th>
<th>Interface</th>
<th>Uptime</th>
<th>Expires</th>
<th>Last</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporter</td>
<td>224.0.1.1</td>
<td>port1.0.1</td>
<td>00:00:09</td>
<td>00:04:17</td>
<td>10.10.0.82</td>
</tr>
<tr>
<td></td>
<td>224.0.1.24</td>
<td>port1.0.2</td>
<td>00:00:06</td>
<td>00:04:14</td>
<td>10.10.0.84</td>
</tr>
<tr>
<td></td>
<td>224.0.1.40</td>
<td>port1.0.3</td>
<td>00:00:09</td>
<td>00:04:15</td>
<td>10.10.0.91</td>
</tr>
<tr>
<td></td>
<td>224.0.1.60</td>
<td>port1.0.3</td>
<td>00:00:05</td>
<td>00:04:15</td>
<td>10.10.0.7</td>
</tr>
<tr>
<td></td>
<td>224.100.100.100</td>
<td>port1.0.1</td>
<td>00:00:11</td>
<td>00:04:13</td>
<td>10.10.0.91</td>
</tr>
<tr>
<td></td>
<td>228.5.16.8</td>
<td>port1.0.3</td>
<td>00:00:11</td>
<td>00:04:16</td>
<td>10.10.0.91</td>
</tr>
<tr>
<td></td>
<td>228.81.16.8</td>
<td>port1.0.7</td>
<td>00:00:05</td>
<td>00:04:15</td>
<td>10.10.0.91</td>
</tr>
<tr>
<td></td>
<td>228.249.13.8</td>
<td>port1.0.3</td>
<td>00:00:08</td>
<td>00:04:17</td>
<td>10.10.0.91</td>
</tr>
<tr>
<td></td>
<td>235.80.68.83</td>
<td>port1.0.11</td>
<td>00:00:12</td>
<td>00:04:15</td>
<td>10.10.0.40</td>
</tr>
<tr>
<td></td>
<td>239.255.255.250</td>
<td>port1.0.3</td>
<td>00:00:12</td>
<td>00:04:15</td>
<td>10.10.228</td>
</tr>
<tr>
<td></td>
<td>239.255.255.254</td>
<td>port1.0.12</td>
<td>00:00:08</td>
<td>00:04:13</td>
<td>10.10.0.84</td>
</tr>
</tbody>
</table>

Table 25-1:  Parameters in the output of the show ip igmp groups command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>Address of the multicast group.</td>
</tr>
<tr>
<td>Interface</td>
<td>Port through which the group is reachable.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The time in weeks, days, hours, minutes, and seconds that this multicast group has been known to the device.</td>
</tr>
</tbody>
</table>
Table 25-1: Parameters in the output of the `show ip igmp groups` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expires</td>
<td>Time (in hours, minutes, and seconds) until the entry expires.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>Last host to report being a member of the multicast group.</td>
</tr>
</tbody>
</table>
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.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ip igmp interface [<interface>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>The name of the VLAN interface.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Examples**
The following output shows IGMP interface status for **vlan2** (with IGMP Snooping enabled):

```
awplus#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
awplus(config)#interface vlan2
awplus(config-if)#ip igmp snooping
awplus(config-if)#exit
awplus(config)#exit
awplus#show ip igmp interface vlan2
Interface vlan2 (Index 202)
   IGMP Disabled, Inactive, Version 3 (default)
   IGMP interface has 0 group-record states
   IGMP activity: 0 joins, 0 leaves
   IGMP robustness variable is 2
   IGMP last member query count is 2
   IGMP query interval is 125 seconds
   IGMP query holdtime is 500 milliseconds
   IGMP querier timeout is 255 seconds
   IGMP max query response time is 10 seconds
   Last member query response interval is 1000 milliseconds
   Group Membership interval is 260 seconds
   Strict IGMPv3 ToS checking is disabled on this interface
   Source Address checking is enabled
   IGMP Snooping is globally enabled
   IGMP Snooping query solicitation is globally disabled
   Num. query-solicit packets: 57 sent, 0 recvd
   IGMP Snooping is enabled on this interface
   IGMP Snooping fast-leave is not enabled
   IGMP Snooping querier is not enabled
   IGMP Snooping report suppression is enabled
awplus#
```
The following output shows IGMP interface status for **vlan2** (with IGMP Snooping disabled):

```
awplus#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
awplus(config)#interface vlan2
awplus(config-if)#no ip igmp snooping
awplus(config-if)#exit
awplus(config)#exit
awplus#show ip igmp interface vlan2
Interface vlan2 (Index 202)
  IGMP Disabled, Inactive, Version 3 (default)
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP robustness variable is 2
  IGMP last member query count is 2
  IGMP query interval is 125 seconds
  IGMP query holdtime is 500 milliseconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
  Strict IGMPv3 ToS checking is disabled on this interface
  Source Address checking is enabled
  IGMP Snooping is globally enabled
  IGMP Snooping query solicitation is globally disabled
  Num. query-solicit packets: 57 sent, 0 recvd
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
awplus#
```

The following command displays the IGMP interface status and Query Solicitation for **vlan3**:
IGMP AND IGMP SNOOPING COMMANDS
SHOW IP IGMP INTERFACE

NOTE: Query Solicitation status information is highlighted in **bold** in the above output.

Use the `show ip igmp interface` command to validate that Query Solicitation is enabled and to show the number of query-solicit message packets sent and received on a VLAN.
**Related Commands**

clear ip igmp
clear ip igmp group
clear ip igmp interface
ip igmp
ip igmp last-member-query-count
ip igmp last-member-query-interval
ip igmp querier-timeout
ip igmp query-holdtime
ip igmp query-interval
ip igmp query-max-response-time
ip igmp robustness-variable
ip igmp snooping
ip igmp snooping fast-leave
ip igmp snooping querier
ip igmp snooping report-suppression
ip igmp snooping tcn query solicit
ip igmp version
**show ip igmp 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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ip igmp proxy
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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>Specify IGMP proxy group membership information.</td>
</tr>
<tr>
<td>detail</td>
<td>Specify detailed IGMPv3 source information.</td>
</tr>
<tr>
<td>&lt;vlan&gt;</td>
<td>Specify the name of a single VLAN interface, for example <strong>vlan1</strong>.</td>
</tr>
<tr>
<td>&lt;multicast-group&gt;</td>
<td>Specify the IPv4 address in of the multicast group, in the format A.B.C.D.</td>
</tr>
</tbody>
</table>

**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
```

To display the state of IGMP Proxy services for VLAN interface **vlan1**, enter the command:
```
awplus# show ip igmp proxy groups vlan1
```

To display the detailed state of IGMP Proxy services for VLAN interface **vlan1**, enter the command:
```
awplus# show ip igmp proxy groups vlan1 detail
```

**Related Commands**
ip igmp proxy-service
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ip igmp snooping mrouter [interface <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 25-3:** Example output from the show ip igmp snooping mrouter command

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Interface</th>
<th>Static/Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>port1.0.5</td>
<td>Statically configured</td>
</tr>
<tr>
<td>200</td>
<td>port1.0.2</td>
<td>Statically configured</td>
</tr>
</tbody>
</table>

**Figure 25-4:** Example output from the show ip igmp snooping mrouter interface vlan1 command

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Interface</th>
<th>Static/Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>port1.0.5</td>
<td>Statically configured</td>
</tr>
</tbody>
</table>

**Related Commands**

ip igmp snooping mrouter
show ip igmp snooping routermode

**Overview**
Use this command to display the current routermode 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 “Controlling “show” Command Output” in 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 routermode and the list of router multicast addresses, use the command:

```
awplus# show ip igmp snooping routermode
```

**Output**
Figure 25-5: Example output from the `show ip igmp snooping routermode` command

```
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
show ip igmp snooping statistics

**Overview**
Use this command to display IGMP Snooping statistics data.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ip igmp snooping statistics interface <interface-range> [group [<ip-address>]]
```

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>Optionally specify the address of the multicast group, entered in the form A.B.C.D.</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>Specify the name of the VLAN interface or interface range.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Example**
To display IGMP statistical information for vlan1 and vlan2, use the command:
```
awplus# show ip igmp snooping statistics interface vlan1-vlan2
```

**Output**
Figure 25-6: Example output from the `show ip igmp snooping statistics` command

```
IGMP Snooping statistics for vlan1
Interface: port1.0.3
Group: 224.1.1.1
Uptime: 00:00:09
Group mode: Exclude (Expires: 00:04:10)
Last reporter: 10.4.4.5
Source list is empty

IGMP Snooping statistics for vlan2
Interface: port1.0.4
Group: 224.1.1.2
Uptime: 00:00:19
Group mode: Exclude (Expires: 00:05:10)
Last reporter: 10.4.4.6
Source list is empty
```
**unddebug igmp**

**Overview**  This command applies the functionality of the no debug igmp command.
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.

NOTE:

MLD and MLD Snooping commands only apply to switch ports, not ETH interfaces.

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.

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.
MLD AND MLD SNOOPING COMMANDS

Command List

- “clear ipv6 mld” on page 1124
- “clear ipv6 mld group” on page 1125
- “clear ipv6 mld interface” on page 1126
- “debug mld” on page 1127
- “ipv6 mld” on page 1130
- “ipv6 mld access-group” on page 1131
- “ipv6 mld immediate-leave” on page 1132
- “ipv6 mld last-member-query-count” on page 1133
- “ipv6 mld last-member-query-interval” on page 1134
- “ipv6 mld limit” on page 1135
- “ipv6 mld querier-timeout” on page 1137
- “ipv6 mld query-interval” on page 1138
- “ipv6 mld query-max-response-time” on page 1139
- “ipv6 mld robustness-variable” on page 1140
- “ipv6 mld snooping” on page 1141
- “ipv6 mld snooping fast-leave” on page 1143
- “ipv6 mld snooping mrouter” on page 1144
- “ipv6 mld snooping querier” on page 1146
- “ipv6 mld snooping report-suppression” on page 1147
- “ipv6 mld static-group” on page 1149
- “ipv6 mld version” on page 1151
- “show debugging mld” on page 1152
- “show ipv6 mld groups” on page 1153
- “show ipv6 mld interface” on page 1154
- “show ipv6 mld snooping mrouter” on page 1155
- “show ipv6 mld snooping statistics” on page 1156
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> }

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Clears all groups on all interfaces. This is an alias to the clear ipv6 mld command.</td>
</tr>
<tr>
<td>&lt;ipv6-address&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>Specifies name of the interface; all groups learned from this interface are deleted.</td>
</tr>
</tbody>
</table>

- **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}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Debug all MLD.</td>
</tr>
<tr>
<td>decode</td>
<td>Debug MLD decoding.</td>
</tr>
<tr>
<td>encode</td>
<td>Debug MLD encoding.</td>
</tr>
<tr>
<td>events</td>
<td>Debug MLD events.</td>
</tr>
<tr>
<td>fsm</td>
<td>Debug MLD Finite State Machine (FSM).</td>
</tr>
<tr>
<td>tib</td>
<td>Debug MLD Tree Information Base (TIB).</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec and Global Configuration

**Usage**  
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
```
MLD AND MLD SNOOPING COMMANDS
DEBUG MLD

**Output**

Warning: Console logging enabled
awplus#05:15:00 awplus NSM[1406]: [MLD-DECODE] Dec V2 Grp Rec: Grp ff08::1 on port2.0.1
05:15:00 awplus NSM[1406]: [MLD-DECODE] Dec V2 Grp Rec: G-Rec not found! on port2.0.1 for ff08::1
05:15:00 awplus NSM[1406]: [MLD-DECODE] Process Event: I=port2.0.1, G=ff08::1, State: Include, Event: Change To Include
05:15:00 awplus NSM[1406]: [MLD-FSM] State Change: Include(1)->Include(1)
05:15:00 awplus NSM[1406]: [MLD-ENCODE] Send Grp - Src Report: HST-IF vlan1: No Router Ports found
05:15:00 awplus NSM[1406]: [MLD-DECODE] Socket Read: Ignoring MLD Message on L3 sockets since Snooping is enabled on vlan1
05:15:01 awplus NSM[1406]: [MLD-DECODE] Dec V2 Grp Rec: Grp ff08::1 on port2.0.1
05:15:01 awplus NSM[1406]: [MLD-ENCODE] MLD Enc Hdr: MLD Listener Query Checksum =8511, MsgLen=60
05:15:01 awplus NSM[1406]: [MLD-ENCODE] Send Group - Source Query: Sent G-S Query on port2.0.1
05:15:01 awplus NSM[1406]: [MLD-FSM] State Change: Include(1)->Exclude(2)
05:15:01 awplus NSM[1406]: [MLD-TIB] Source Rec Del: S=2002::3 Intf=vlan1
05:15:01 awplus NSM[1406]: [MLD-ENCODE] Send Group Report: HST-IF vlan1: No Router Ports found
05:15:01 awplus NSM[1406]: [MLD-DECODE] Socket Read: Ignoring MLD Message on L3 sockets since Snooping is enabled on vlan1
05:15:01 awplus NSM[1406]: [MLD-EVENTS] Grp - Src Report Rexmit: Expiry for Grp ff08::1 on vlan1
05:15:02 awplus NSM[1406]: [MLD-EVENTS] Grp - Src Query Rexmit: Expiry for Grp ff08::1 on port2.0.1
05:15:02 awplus NSM[1406]: [MLD-ENCODE] MLD Enc Hdr: MLD Listener Query Checksum=8511, MsgLen=60
05:15:02 awplus NSM[1406]: [MLD-ENCODE] Send Group - Source Query: Sent G-S Query on port2.0.1
05:15:02 awplus NSM[1406]: [MLD-EVENTS] Grp Report Rexmit: Expiry for Grp ff08::1 on vlan1
05:15:02 awplus NSM[1406]: [MLD-ENCODE] Send Group Report: HST-IF vlan1: No Router Ports found
MLD AND MLD SNOOPING COMMANDS

DEBUG MLD

Related Commands

show debugging mld

ff08::1 on vlan1
05:15:02 awplus NSM[1406]: [MLD-TIB] Source Rec Del: S=2002::3 Intf=vlan1
05:15:03 awplus NSM[1406]: [MLD-EVENTS] Src - Rec Liveness Timer: Expiry for Src
2002::3 on port2.0.1
00:15:03 awplus NSM[1406]: [MLD-FSM] Process Event: I=port2.0.1, G=ff08::1,
State: Exclude, Event: Source Tmr Expiry
05:15:03 awplus NSM[1406]: [MLD-FSM] State Change: Exclude(2) -> Exclude(2)
05:15:03 awplus NSM[1406]: [MLD-FSM] Host Process Event: I=vlan1, G=ff08::1,
05:15:06 awplus appmond[1244]: monitoring imi memory usage (max:51200000 kB)
05:15:06 awplus appmond[1244]: monitoring rmond memory usage (max:51200000 kB)
05:15:06 awplus appmond[1244]: monitoring lldpd memory usage (max:51200000 kB)
05:15:06 awplus NSM[1406]: [MLD-EVENTS] Querier Timer: Expiry on port2.0.1, Sending General Query
05:15:06 awplus NSM[1406]: [MLD-ENCODE] MLD Enc Hdr: MLD Listener Query Checksum
-14706, MsgLen=28
05:15:06 awplus NSM[1406]: [MLD-ENCODE] Send Gen Query: Sent General Query on
port2.0.1, ret=90
05:15:06 awplus NSM[1406]: [MLD-EVENTS] Querier Timer: Expiry on port2.0.1,
Sending General Query
05:15:06 awplus NSM[1406]: [MLD-ENCODE] MLD Enc Hdr: MLD Listener Query Checksum
-14706, MsgLen=28
05:15:06 awplus NSM[1406]: [MLD-ENCODE] Send Gen Query: Sent General Query on
port2.0.1, ret=90
05:15:06 awplus NSM[1406]: [MLD-EVENTS] Querier Timer: Expiry on port2.0.1,
Sending General Query
05:15:06 awplus NSM[1406]: [MLD-ENCODE] MLD Enc Hdr: MLD Listener Query Checksum
-14706, MsgLen=28
05:15:06 awplus NSM[1406]: [MLD-ENCODE] Send Gen Query: Sent General Query on port2.0.1, ret=90
MLD AND MLD SNOOPING COMMANDS

IPV6 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.

x510 series switches have a 128 MLD group limit for (*, G) and (S,G) entries.

There is a 100 MLD interface limit when applying MLD commands to multiple VLANs. Only the first 100 VLANs have the required multicast structures added to the interfaces that allow multicast routing.

The device has a 512 MLD group limit for (*, G) and (S,G) entries.

Syntax
ipv6 mld
no ipv6 mld

Default
MLD is disabled by default.

Mode
Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage
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
**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
```

**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**  
```plaintext
ipv6 mld immediate-leave group-list <IPv6-access-list-name>
no ipv6 mld immediate-leave
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `<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:

```plaintext
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;value&gt;</td>
<td>Count value. Valid values are from 2 to 7.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;milliseconds&gt;</code></td>
<td>The time delay between successive query messages (in milliseconds). Valid values are from 1000 to 25500 milliseconds.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Description</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;limitvalue&gt;</code></td>
<td><code>&lt;2-512&gt;</code> Maximum number of group membership states.</td>
</tr>
<tr>
<td><code>&lt;IPv6-access-list-name&gt;</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Default**
The default limit, which is reset by the `no` variant of this command, is the same as maximum number of group membership entries that can be learned with the `ipv6 mld limit` command.

The default limit of group membership entries that can be learned is 512 entries.

**Mode**
Global Configuration and Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

**Usage**
This command applies to interfaces configured for MLD Layer-3 multicast protocols and learned by MLD Snooping.

**Examples**
The following example configures an MLD limit of 100 group-memberships across all VLAN interfaces on which MLD is enabled, and excludes groups in the range `ff1e:0db8:0001::/64` from this limitation:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard v6grp permit ff1e:0db8:0001::/64
awplus(config)# ipv6 mld limit 100 except v6grp
```
The following example configures an MLD limit of 100 group-membership states on the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld limit 100
```

The following example configures an MLD limit of 100 group-membership states on the VLAN interfaces vlan2-vlan4:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld limit 100
```

`show ipv6 mld groups`
ipv6 mld 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;seconds&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Default**
255 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 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
```

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;seconds&gt;</code></td>
<td>Maximum response time (in seconds) advertised in MLD queries. Valid values are from 1 to 240 seconds.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;value&gt;</td>
<td>Valid values are from 1 to 7.</td>
</tr>
</tbody>
</table>

**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.

x510 series switches have a 128 MLD group limit for (*, G) and (S,G) entries.

There is a 100 MLD interface limit when applying MLD commands to multiple VLANs. Only the first 100 VLANs have the required multicast structures added to the interfaces that allow multicast routing.

The device has a 512 MLD group limit for (*, G) and (S,G) entries.

**Syntax**
ipv6 mld snooping
no ipv6 mld snooping

**Default**
By default, MLD Snooping is enabled both globally and on all VLANs.

**Mode**
Global Configuration and Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

**Usage**
For MLD Snooping to operate on particular VLAN interfaces, it must be enabled both globally by using this command in Global Configuration mode, and on individual VLAN interfaces by using this command in Interface Configuration mode (both are enabled by default).

MLD requires memory for storing data structures, as well as the hardware tables to implement hardware routing. As the number of ports, VLANs, static and dynamic groups increases then more memory is consumed. You can track the memory used for MLD with the command:

```
awplus# show memory pools nsm | grep MLD
```

Static and dynamic groups (LACP), ports and VLANs are not limited for MLD. For VLANs, this allows you to configure MLD across more VLANs with fewer ports per VLAN, or fewer VLANs with more ports per VLAN. For LACPs, you can configure MLD across more LACP groups with fewer ports per LACP, or fewer LACP groups with more ports per LACP.
Examples

To configure MLD Snooping on the VLAN interface `vlan2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping
```

To configure MLD Snooping on the VLAN interfaces `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 interface `vlan2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config)# no ipv6 mld snooping
```

To disable MLD Snooping for the VLAN interfaces `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**  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>
nov6 mld snooping mrouter interface <port>
```

**Mode**
Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

**Usage**
This MLD Snooping command statically configures a switch port as a Multicast Router interface.

Note that if static IPv6 multicast routing is being used with EPSR and the destination VLAN is an EPSR data VLAN, then multicast router (mrouter) ports must be statically configured. This minimizes disruption for multicast traffic in the event of ring failure or restoration.

When configuring the EPSR data VLAN, statically configure mrouter ports so that the multicast router can be reached in either direction around the EPSR ring.

For example, if port1.0.1 and port1.0.6 are ports on an EPSR data VLAN vlan101, which is the destination for a static IPv6 multicast route, then configure both ports as multicast router (mrouter) ports as shown in the example commands listed below:

**Output**
Figure 26-1: 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
```
MLD AND MLD SNOOPING COMMANDS
IPV6 MLD SNOOPING MROUTER

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 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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipv6-group-address&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;ipv6-source-address&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>ssm-map</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

Mode
Interface Configuration for a VLAN interface.

Usage
This command applies to MLD Snooping on a VLAN interface to statically add groups and/or source records.
MLD AND MLD SNOOPING COMMANDS

IPV6 MLD STATIC-GROUP

Examples

The following examples show how to statically add group and/or source records for MLD:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source fe80::2fd:6cff:fe1c:b
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source ssm-map
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source ssm-map interface port1.0.4
```

The following examples show how to statically add group and/or source records for MLD Snooping on VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source fe80::2fd:6cff:fe1c:b
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source ssm-map
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source ssm-map interface port1.0.4
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source fe80::2fd:6cff:fe1c:b interface port1.0.4
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source ssm-map interface port1.0.4
```
**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**  This command applies to interfaces configured for MLD Layer-3 multicast protocols, 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 display the MLD debugging modes enabled with the debug mld command.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show debugging mld

**Mode**  Privileged Exec

**Example**  
awplus# show debugging mld

**Output**

```
show debugging mld
MLD Debugging status:
   MLD Decoder debugging is on
   MLD Encoder debugging is on
   MLD Events debugging is on
   MLD FSM debugging is on
   MLD Tree-Info-Base (TIB) debugging is on
```

**Related Commands**  debug mld
show ipv6 mld groups

**Overview**  
Use this command to display the multicast groups with receivers directly connected to the router, and learned through MLD.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show ipv6 mld groups [\<ipv6-address\> |\<interface\>] [detail]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipv6-address&gt;</td>
<td>Optional. Specify Address of the multicast group in format X::X::X.</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>Optional. Specify the Interface name for which to display local information.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Examples**  
The following command displays local-membership information for all interfaces:

```
awplus# show ipv6 mld groups
```

**Output**

MLD Connected Group Membership

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Interface</th>
<th>Uptime</th>
<th>Expires</th>
<th>Last Reporter</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff08::1</td>
<td>port1.0.1</td>
<td>00:00:24</td>
<td>stopped</td>
<td>fe80::eecd:6dff:fe6b:4783</td>
</tr>
</tbody>
</table>

The following command displays local-membership information for all interfaces:

```
awplus# show ipv6 mld groups detail
```

**Output**

MLD Connected Group Membership Details for port1.0.1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Group</th>
<th>Uptime</th>
<th>Group mode</th>
<th>Last reporter</th>
<th>Group source list: (R - Remote, M - SSM Mapping, S - Static)</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.1</td>
<td>ff08::1</td>
<td>00:00:13</td>
<td>Include ()</td>
<td>fe80::eecd:6dff:fe6b:4783</td>
<td>(R - Remote, M - SSM Mapping, S - Static)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Uptime</th>
<th>v2 Exp</th>
<th>Fwd</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8::1</td>
<td>00:00:13</td>
<td>00:04:07</td>
<td>Yes</td>
<td>R</td>
</tr>
<tr>
<td>2002:db8::3</td>
<td>00:00:13</td>
<td>00:04:07</td>
<td>Yes</td>
<td>R</td>
</tr>
</tbody>
</table>
**show ipv6 mld interface**

**Overview**  
Use this command to display the state of MLD and MLD Snooping for a specified interface, or all interfaces.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
`show ipv6 mld interface [<interface>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>Interface name.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Example**  
The following command displays MLD interface status on all interfaces enabled for MLD:

```plaintext
awplus# show ipv6 mld interface
```

**Output**

```plaintext
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ipv6 mld snooping mrouter [<interface>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>Optional. Specify the name of the VLAN interface. Note: If you do not specify a single VLAN interface, then all VLAN interfaces are shown.</td>
</tr>
</tbody>
</table>

**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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
show ipv6 mld snooping statistics interface <interface>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>The name of the VLAN interface.</td>
</tr>
</tbody>
</table>

**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
```
27 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.
PIM-SM COMMANDS

Command List

- “clear ip pim sparse-mode bsr rp-set *” on page 1159
- “clear ip mroute pim sparse-mode” on page 1160
- “debug pim sparse-mode” on page 1161
- “debug pim sparse-mode timer” on page 1162
- “ip pim accept-register list” on page 1164
- “ip pim anycast-rp” on page 1165
- “ip pim bsr-border” on page 1166
- “ip pim bsr-candidate” on page 1167
- “ip pim cisco-register-checksum” on page 1168
- “ip pim cisco-register-checksum group-list” on page 1169
- “ip pim crp-cisco-prefix” on page 1170
- “ip pim dr-priority” on page 1171
- “ip pim exclude-genid” on page 1172
- “ip pim ext-srscs-directly-connected (PIM-SM)” on page 1173
- “ip pim hello-holdtime (PIM-SM)” on page 1174
- “ip pim hello-interval (PIM-SM)” on page 1175
- “ip pim ignore-rp-set-priority” on page 1176
- “ip pim jp-timer” on page 1177
- “ip pim neighbor-filter (PIM-SM)” on page 1178
- “ip pim register-rate-limit” on page 1179
- “ip pim register-rp-reachability” on page 1180
- “ip pim register-source” on page 1181
- “ip pim register-suppression” on page 1182
- “ip pim rp-address” on page 1183
- “ip pim rp-candidate” on page 1185
- “ip pim rp-register-kat” on page 1186
- “ip pim sparse-mode” on page 1187
- “ip pim sparse-mode passive” on page 1188
- “ip pim spt-threshold” on page 1189
- “ip pim spt-threshold group-list” on page 1190
- “ip pim ssm” on page 1191
- “show debugging pim sparse-mode” on page 1192
- “show ip pim sparse-mode bsr-router” on page 1193
- “show ip pim sparse-mode interface” on page 1194
- “show ip pim sparse-mode interface detail” on page 1196
PIM-SM COMMANDS

- “show ip pim sparse-mode local-members” on page 1197
- “show ip pim sparse-mode mroute” on page 1199
- “show ip pim sparse-mode mroute detail” on page 1201
- “show ip pim sparse-mode neighbor” on page 1203
- “show ip pim sparse-mode nexthop” on page 1204
- “show ip pim sparse-mode rp-hash” on page 1205
- “show ip pim sparse-mode rp mapping” on page 1206
- “undebug all pim sparse-mode” on page 1207
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 *

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Clears all RP sets.</td>
</tr>
</tbody>
</table>

**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 ip pim sparse-mode bsr rp-set *
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Group-IP-address&gt;</td>
<td>Specify a multicast group IPv6 address, entered in the form A.B.C.D.</td>
</tr>
<tr>
<td>&lt;Source-IP-address&gt;</td>
<td>Specify a source group IP address, entered in the form A.B.C.D.</td>
</tr>
</tbody>
</table>

**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
**debug pim sparse-mode**

**Overview**
Use this command to activate/de-activate all PIM-SM debugging.

**Syntax**
```
depug 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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Activates/deactivates all PIM-SM debugging.</td>
</tr>
<tr>
<td>events</td>
<td>Activates debug printing of events.</td>
</tr>
<tr>
<td>mfc</td>
<td>Activates debug printing of MFC (Multicast Forwarding Cache in kernel) add/delete/updates.</td>
</tr>
<tr>
<td>mib</td>
<td>Activates debug printing of PIM-SM MIBs.</td>
</tr>
<tr>
<td>nexthop</td>
<td>Activates debug printing of PIM-SM next hop communications.</td>
</tr>
<tr>
<td>nsm</td>
<td>Activates debugging of PIM-SM Network Services Module communications.</td>
</tr>
<tr>
<td>packet</td>
<td>Activates debug printing of incoming and/or outgoing packets.</td>
</tr>
<tr>
<td>state</td>
<td>Activates debug printing of state transition on all PIM-SM FSMs.</td>
</tr>
<tr>
<td>mtrace</td>
<td>Activates debug printing of multicast traceroute.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec and Global Configuration

**Example**
```
awplus# configure terminal
awplus(config)# debug pim sparse-mode all
```

**Related Commands**
*show debugging pim sparse-mode*

*undebug all pim sparse-mode*
**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**
```plaintext
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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assert</td>
<td>Enable or disable debugging for the Assert timers.</td>
</tr>
<tr>
<td>at</td>
<td>Enable or disable debugging for the Assert Timer.</td>
</tr>
<tr>
<td>bsr</td>
<td>Enable or disable debugging for the specified Bootstrap Router timer, or all Bootstrap Router timers.</td>
</tr>
<tr>
<td>bst</td>
<td>Enable or disable debugging for the Bootstrap Router: Bootstrap Timer.</td>
</tr>
<tr>
<td>crp</td>
<td>Enable or disable debugging for the Bootstrap Router: Candidate-RP Timer.</td>
</tr>
<tr>
<td>hello</td>
<td>Enable or disable debugging for the specified Hello timer, or all Hello timers.</td>
</tr>
<tr>
<td>ht</td>
<td>Enable or disable debugging for the Hello timer: Hello Timer.</td>
</tr>
<tr>
<td>nlt</td>
<td>Enable or disable debugging for the Hello timer: Neighbor Liveness Timer.</td>
</tr>
<tr>
<td>tht</td>
<td>Enable or disable debugging for the Hello timer: Triggered Hello Timer.</td>
</tr>
<tr>
<td>joinprune</td>
<td>Enable or disable debugging for the specified JoinPrune timer, or all JoinPrune timers.</td>
</tr>
<tr>
<td>jt</td>
<td>Enable or disable debugging for the JoinPrune timer: upstream Join Timer.</td>
</tr>
<tr>
<td>et</td>
<td>Enable or disable debugging for the JoinPrune timer: Expiry Timer.</td>
</tr>
<tr>
<td>ppt</td>
<td>Enable or disable debugging for the JoinPrune timer: PrunePending Timer.</td>
</tr>
<tr>
<td>kat</td>
<td>Enable or disable debugging for the JoinPrune timer: KeepAlive Timer.</td>
</tr>
</tbody>
</table>
### Debug PIM Sparse-Mode Timer

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ot</td>
<td>Enable or disable debugging for the JoinPrune timer: Upstream Override Timer.</td>
</tr>
<tr>
<td>register</td>
<td>Enable or disable debugging for the Register timers.</td>
</tr>
<tr>
<td>rst</td>
<td>Enable or disable debugging for the Register timer: Register Stop Timer.</td>
</tr>
</tbody>
</table>

**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
**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. By default, the RP accepts register packets from all multicast sources.

Use the **no** variant of this command to revert to default.

**Syntax**
```
ip pim accept-register
list(<simplerange>|<exprange>|<access-list>)
no ip pim accept-register
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;simplerange&gt;</td>
<td>&lt;100-199&gt; IP extended access-list.</td>
</tr>
<tr>
<td>&lt;exprange&gt;</td>
<td>&lt;2000-2699&gt; IP extended access list (expanded range).</td>
</tr>
<tr>
<td>&lt;access-list&gt;</td>
<td>IP Named Standard Access list.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Example**
```
awplus# configure terminal
awplus(config)# ip pim accept-register list 121
awplus(config)# access-list 121 permit ip 100.1.1.1 0.0.0.0 any
```
**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> ]
```

**Mode**
Global Configuration

**Usage**
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 `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
```
**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**

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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>The interface. For instance, vlan2.</td>
</tr>
<tr>
<td>&lt;hash&gt;</td>
<td>&lt;0-32&gt; configure hash mask length for RP selection. The default hash value if you do not configure this parameter is 10.</td>
</tr>
<tr>
<td>&lt;priority&gt;</td>
<td>&lt;0-255&gt; configure priority for a BSR candidate. Note that you must also specify the &lt;hash&gt; (mask length) when specifying the &lt;priority&gt;. The default priority if you do not configure this parameter is 64.</td>
</tr>
</tbody>
</table>

**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
```
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
```
**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
[<simplerange>|<exprange>|<access-list>]
```

```
no ip pim cisco-register-checksum group-list
[<simplerange>|<exprange>|<access-list>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;simplerange&gt;</td>
<td>&lt;1-99&gt; Simple access-list.</td>
</tr>
<tr>
<td>&lt;exprange&gt;</td>
<td>&lt;1300-1999&gt; Simple access-list (expanded range).</td>
</tr>
<tr>
<td>&lt;access-list&gt;</td>
<td>IP Named Standard Access list.</td>
</tr>
</tbody>
</table>

**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
```
**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**  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`
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>]
```

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| <priority> | <0-4294967294>  
The Designated Router priority value.  
A higher value has a higher preference. |
**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**
```
aplus# configure terminal
applus(config)# interface vlan2
applus(config-if)# ip pim exclude-genid
```
ip pim ext-srcs-directly-connected (PIM-SM)

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;holdtime&gt;</td>
<td>&lt;1-65535&gt;</td>
</tr>
<tr>
<td></td>
<td>The holdtime value in seconds (no fractional seconds are accepted).</td>
</tr>
</tbody>
</table>

**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
```
**PIM-SM COMMANDS**

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interval&gt;</td>
<td>&lt;1-65535&gt; The value in seconds (no fractional seconds accepted).</td>
</tr>
</tbody>
</table>

**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>]
```

**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
```
**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>}
nop ip pim neighbor-filter {<number>|<accesslist>}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;number&gt;</code></td>
<td>&lt;1-99&gt; Standard IP access-list number.</td>
</tr>
<tr>
<td><code>&lt;accesslist&gt;</code></td>
<td>IP access list name.</td>
</tr>
</tbody>
</table>

**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**
```bash
ip pim register-rate-limit <1-65535>
no ip pim register-rate-limit
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Specifies the maximum number of packets that can be sent per second.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Example**
```bash
awplus# configure terminal
awplus(config)# ip pim register-rate-limit 3444
```
**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
**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;source_address&gt;</code></td>
<td>The IP address, entered in the form A.B.C.D, to be used as the source of the register packets.</td>
</tr>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>The name of the interface to be used as the source of the register packets.</td>
</tr>
</tbody>
</table>

**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 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
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>Register suppression on time in seconds.</td>
</tr>
</tbody>
</table>

**Mode** Global Configuration

**Example**

```
awplus# configure terminal
awplus(config)# ip pim register-suppression 192
```
ip pim rp-address

**Overview**
Use this command to statically configure RP (Rendezvous Point) address for multicast groups.

Use the no variant of this command to remove a statically configured RP (Rendezvous Point) address for multicast groups.

**Syntax**
```
ip pim rp-address <ip-address> [ <simplerange> | <expandedrange> | <accesslist> ] [ <override> ]
no ip pim rp-address <ip-address> [ <simplerange> | <expandedrange> | <accesslist> ] [ <override> ]
```

**Mode**
Global Configuration

**Usage**
The AlliedWare Plus™ PIM-SM implementation supports multiple static RPs. It also supports usage of static-RP and BSR 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 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 Access Lists. However, configuring multiple static RPs (using `ip 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 `224.0.0.0/4` (without ACL) or for specific group ranges (using ACL).

For example, configuring `ip pim rp-address 192.168.3.4` will configure static-RP 192.168.3.4 for the default group range 224.0.0.0/4. Configuring `ip pim rp-address 192.168.7.8 grp-list` will configure static-RP 192.168.7.8 for all the group ranges represented by permit filters in grp-list ACL.

If multiple static-RPs are available for a group range, then one with the highest IP address is chosen.
Only Permit filters in ACL are considered as valid group ranges. The default Permit filter 0.0.0.0/0 is converted to the default multicast filter 224.0.0.0/4.

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.

Group mode and RP address mappings learned through BSR take precedence over mappings statistically defined by the `ip pim rp-address` command. Commands with the override keyword take precedence over dynamically learned mappings.

**Example**

```
awplus# configure terminal
awplus(config)# ip pim rp-address 192.168.3.4 4
```

**Related Commands**

- `ip pim rp-candidate`
- `ip pim rp-register-kat`
**ip pim rp-candidate**

**Overview**
Use this command to give the router the candidate RP (Rendezvous Point) status 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).
<grouplist> | IP access list specifier for standard, expanded or named access lists in their respective ranges: [1-99] [WORD]

**Default**
The priority value for a candidate RP is 192 by default until specified using the **priority** parameter.

**Mode**
Global Configuration

**Usage**
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 192.

**Examples**
```
awplus# configure terminal
awplus(config)# ip pim rp-candidate vlan2 priority 3
awplus# configure terminal
awplus(config)# ip pim rp-candidate vlan2 priority 3 group-list 3
awplus# configure terminal
awplus(config)# no ip pim rp-candidate vlan2
```

**Related Commands**
- **ip pim rp-address**
- **ip pim rp-register-kat**
**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
```

**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

**Parameter** | **Description**
--- | ---
<1-65536> | Specify the KAT timer in seconds. The default value is 210 seconds.
**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 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 spt-threshold**

**Overview**  This command turns on the ability for the last-hop PIM router to switch to SPT.  
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**  
awplus# configure terminal  
awplus(config)# ip pim spt-threshold  
awplus# configure terminal  
awplus(config)# no ip pim spt-threshold
ip pim spt-threshold group-list

**Overview**
Use this command to 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.

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 {<simplerange>|<expandedrange>|<named-accesslist>}
no ip pim spt-threshold group-list
[<simplerange>|<expandedrange>|<named-accesslist>]
```

**Mode**
Global Configuration

**Usage**
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
```
**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
```

**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
```
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 “Controlling “show” Command Output” in 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 27-1:  Output from the show debugging pim sparse-mode command

```
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
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 “Controlling “show” Command Output” in 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 27-2:  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
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 “Controlling “show” Command Output” in 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**

```
Total configured interfaces: 16   Maximum allowed: 31
Total active interfaces:     12

Address    Interface VIFindex Ver/Mode Nbr Count   DR  DR
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 27-1: Parameters in the output from the show ip pim sparse-mode interface command**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total configured interfaces</td>
<td>The number of configured PIM Sparse Mode interfaces.</td>
</tr>
<tr>
<td>Maximum allowed</td>
<td>The maximum number of PIM Sparse Mode interfaces that can be configured.</td>
</tr>
<tr>
<td>Total active interfaces</td>
<td>The number of active PIM Sparse Mode interfaces.</td>
</tr>
<tr>
<td>Address</td>
<td>Primary PIM-SM address.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the PIM-SM interface.</td>
</tr>
<tr>
<td>VIF Index</td>
<td>The Virtual Interface index of the VLAN.</td>
</tr>
<tr>
<td>Ver/Mode</td>
<td>PIM version/Sparse mode.</td>
</tr>
<tr>
<td>Nbr Count</td>
<td>Neighbor count of the PIM-SM interface.</td>
</tr>
</tbody>
</table>
Table 27-1: Parameters in the output from the **show ip pim sparse-mode interface** command (cont.)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR Priority</td>
<td>Designated Router priority.</td>
</tr>
<tr>
<td>DR</td>
<td>The IP address of the Designated Router.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `ip pim sparse-mode`
- `show ip pim sparse-mode rp mapping`
- `show ip pim sparse-mode neighbor`
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 “Controlling “show” Command Output” in 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 27-3: 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
```
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show ipv6 pim sparse-mode local-members [<interface>]

**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 ipv6 pim sparse-mode local-members
```

**Output**  Figure 27-4: Example output from the `show ip pim sparse-mode local-members` command

```
awplus# show ipv6 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-SMv6 information for the PIM-SM configured interface `vlan1`, use the command:

```
awplus# show ipv6 pim sparse-mode local-members vlan1
```
Output  Figure 27-5: 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
```
show ip pim sparse-mode mroute

**Overview**  This command displays the IP multicast routing table, or the IP multicast routing table based on the specified address or addresses.

Two group addresses cannot be used simultaneously; two source addresses cannot be used simultaneously.

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.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  

```
show ip pim sparse-mode mroute
[<group-address>|<source-address>]
show ip pim sparse-mode mroute [<source-address> <group-address>]
show ip pim sparse-mode mroute [<group-address> <source-address>]
```

**Parameter**  

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group IP address, entered in the form A.B.C.D. Based on the group and source address, the output is the selected route if present in the multicast route tree.</td>
</tr>
<tr>
<td>Source IP address, entered in the form A.B.C.D. Based on the source and group address, the output is the selected route if present in the multicast route tree.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Usage**  

Note that when a feature license is enabled, the output for **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.

**Examples**  

```
awplus# show ip pim sparse-mode mroute
awplus# show ip pim sparse-mode mroute 40.40.40.11
awplus# show ip pim sparse-mode mroute 235.0.0.1
awplus# show ip pim sparse-mode mroute 235.0.0.1 40.40.40.11
```
Figure 27-6: Example output from the `show ip pim sparse-mode mroute` command

<table>
<thead>
<tr>
<th>IP Multicast Routing Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>(<em>,</em>,RP) Entries: 0</td>
</tr>
<tr>
<td>(*,G) Entries: 1</td>
</tr>
<tr>
<td>(S,G) Entries: 0</td>
</tr>
<tr>
<td>(S,G,rpt) Entries: 0</td>
</tr>
<tr>
<td>FCR Entries: 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(*, 224.0.1.3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP: 10.10.5.153</td>
</tr>
<tr>
<td>RPF nbr: 192.168.1.152</td>
</tr>
<tr>
<td>RPF idx: vlan2</td>
</tr>
<tr>
<td>Upstream State: JOINED</td>
</tr>
<tr>
<td>Local</td>
</tr>
<tr>
<td>Source: 10.10.1.52</td>
</tr>
</tbody>
</table>
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.

Two group addresses cannot be used simultaneously; two source addresses cannot be used simultaneously.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ip pim sparse-mode mroute
[<group-address>|<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
```

**Usage**
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 27-7: 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
```
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
```
show ip pim sparse-mode neighbor [<interface>] [<ip-address>] [detail]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>Interface name (e.g. vlan2). Show neighbors on an interface.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>Show neighbors with a particular address on an interface. The IP address entered in the form A.B.C.D.</td>
</tr>
<tr>
<td>detail</td>
<td>Show detailed information.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Examples**  
```
awplus# show ip pim sparse-mode neighbor
awplus# show ip pim sparse-mode neighbor vlan5 detail
```

**Figure 27-8:** Example output from the `show ip pim sparse-mode neighbor` command

<table>
<thead>
<tr>
<th>Neighbor Address</th>
<th>Interface</th>
<th>Uptime/Expires</th>
<th>Ver</th>
<th>DR Priority/ Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.9</td>
<td>vlan2</td>
<td>00:55:33/00:01:44</td>
<td>v2</td>
<td>1 /</td>
</tr>
<tr>
<td>10.10.0.136</td>
<td>vlan2</td>
<td>00:55:20/00:01:25</td>
<td>v2</td>
<td>1 /</td>
</tr>
<tr>
<td>10.10.0.172</td>
<td>vlan2</td>
<td>00:55:33/00:01:32</td>
<td>v2</td>
<td>1 / DR</td>
</tr>
<tr>
<td>192.168.0.100</td>
<td>vlan3</td>
<td>00:55:30/00:01:20</td>
<td>v2</td>
<td>N / DR</td>
</tr>
</tbody>
</table>

**Figure 27-9:** 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
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 “Controlling “show” Command Output” in 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 27-10: Example output from the `show ip pim sparse-mode nexthop` command

<p>| Flags: N = New, R = RP, S = Source, U = Unreachable |</p>
<table>
<thead>
<tr>
<th>Destination Type</th>
<th>Nexthop Num</th>
<th>Nexthop Addr</th>
<th>Nexthop IfIndex</th>
<th>Metric</th>
<th>Pref</th>
<th>Refcnt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num</td>
<td>Addr</td>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.0.9</td>
<td>.RS. 1</td>
<td>0.0.0.0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 27-2: Parameters in output of the `show ip pim sparse-mode nexthop` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The destination address for which PIM-SM requires next hop information.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of destination, as indicated by the Flags description. N = New, R= RP, S = Source, U = Unreachable.</td>
</tr>
<tr>
<td>Nexthop Num</td>
<td>The number of next hops to the destination. PIM-SM always uses only 1 next hop.</td>
</tr>
<tr>
<td>Nexthop Addr</td>
<td>The address of the primary next hop gateway.</td>
</tr>
<tr>
<td>Nexthop IfIndex</td>
<td>The interface on which the next hop gateway can be reached.</td>
</tr>
<tr>
<td>Nexthop Name</td>
<td>The name of next hop interface.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric of the route towards the destination.</td>
</tr>
<tr>
<td>Preference</td>
<td>The preference of the route towards destination.</td>
</tr>
<tr>
<td>Refcnt</td>
<td>Only used for debugging.</td>
</tr>
</tbody>
</table>
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
```
show ip pim sparse-mode rp-hash <group-addr>
```  

**Mode**  User Exec and Privileged Exec

**Example**  
```
awplus# show ip pim sparse-mode rp-hash 224.0.1.3
```

Figure 27-11: Output from the `show ip pim sparse-mode rp-hash` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;group-addr&gt;</code></td>
<td>The group address for which to find the RP, entered in the form A.B.C.D.</td>
</tr>
</tbody>
</table>

**RP:** 10.10.11.35  
**Info source:** 10.10.11.35, via bootstrap

**Related Commands**  
`show ip pim sparse-mode rp mapping`
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show ip pim sparse-mode rp mapping

**Mode**  
User Exec and Privileged Exec

**Example**  
awplus# show ip pim sparse-mode rp mapping

Figure 27-12: 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
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**  
ddebug pim sparse-mode
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.

NOTE:

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.
PIM-SMV6 COMMANDS

Command List

- “clear ipv6 mroute pim” on page 1209
- “clear ipv6 mroute pim sparse-mode” on page 1210
- “clear ipv6 pim sparse-mode bsr rp-set *” on page 1211
- “debug ipv6 pim sparse-mode” on page 1212
- “debug ipv6 pim sparse-mode packet” on page 1214
- “debug ipv6 pim sparse-mode timer” on page 1215
- “ipv6 pim accept-register” on page 1217
- “ipv6 pim anycast-rp” on page 1218
- “ipv6 pim bsr-border” on page 1219
- “ipv6 pim bsr-candidate” on page 1220
- “ipv6 pim cisco-register-checksum” on page 1221
- “ipv6 pim cisco-register-checksum group-list” on page 1222
- “ipv6 pim crp-cisco-prefix” on page 1223
- “ipv6 pim dr-priority” on page 1224
- “ipv6 pim exclude-genid” on page 1225
- “ipv6 pim ext-srcsrds-directly-connected” on page 1226
- “ipv6 pim hello-holdtime” on page 1227
- “ipv6 pim hello-interval” on page 1228
- “ipv6 pim ignore-rp-set-priority” on page 1229
- “ipv6 pim jp-timer” on page 1230
- “ipv6 pim neighbor-filter” on page 1231
- “ipv6 pim register-rate-limit” on page 1232
- “ipv6 pim register-rp-reachability” on page 1233
- “ipv6 pim register-source” on page 1234
- “ipv6 pim register-suppression” on page 1235
- “ipv6 pim rp-address” on page 1236
- “ipv6 pim rp-candidate” on page 1238
- “ipv6 pim rp embedded” on page 1240
- “ipv6 pim rp-register-kat” on page 1241
- “ipv6 pim sparse-mode” on page 1242
- “ipv6 pim sparse-mode passive” on page 1243
- “ipv6 pim spt-threshold” on page 1244
- “ipv6 pim spt-threshold group-list” on page 1245
- “ipv6 pim ssm” on page 1246
- “ipv6 pim unicast-bsm” on page 1247
• “show debugging ipv6 pim sparse-mode” on page 1248
• “show ipv6 pim sparse-mode bsr-router” on page 1249
• “show ipv6 pim sparse-mode interface” on page 1250
• “show ipv6 pim sparse-mode interface detail” on page 1252
• “show ipv6 pim sparse-mode local-members” on page 1253
• “show ipv6 pim sparse-mode mroute” on page 1255
• “show ipv6 pim sparse-mode mroute detail” on page 1257
• “show ipv6 pim sparse-mode neighbor” on page 1259
• “show ipv6 pim sparse-mode nexthop” on page 1260
• “show ipv6 pim sparse-mode rp-hash” on page 1261
• “show ipv6 pim sparse-mode rp mapping” on page 1262
• “show ipv6 pim sparse-mode rp nexthop” on page 1263
• “undebug all ipv6 pim sparse-mode” on page 1265
• “undebug ipv6 pim sparse-mode” on page 1266
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Clears all PIM-SMv6 multicast routes. Using this command without this optional operator only deletes the multicast router table entries.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;Group-IPv6-add&gt;</code></td>
<td>Specify a multicast group IPv6 address, entered in the form X::X::X.</td>
</tr>
<tr>
<td><code>&lt;Source-IPv6-add&gt;</code></td>
<td>Specify a source group IPv6 address, entered in the form X::X::X.</td>
</tr>
</tbody>
</table>

**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 *

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Clears all RP sets.</td>
</tr>
</tbody>
</table>

**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**
```
depth 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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Activates/deactivates all PIM-SMv6 debugging.</td>
</tr>
<tr>
<td>events</td>
<td>Activates debug printing of PIM-SMv6 events.</td>
</tr>
<tr>
<td>mfc</td>
<td>Activates debug printing of MFC (Multicast Forwarding Cache).</td>
</tr>
<tr>
<td>mib</td>
<td>Activates debug printing of PIM-SMv6 MIBs.</td>
</tr>
<tr>
<td>nexthop</td>
<td>Activates debug printing of PIM-SMv6 next hop communications.</td>
</tr>
<tr>
<td>nsm</td>
<td>Activates debugging of PIM-SMv6 NSM (Network Services Module) communications.</td>
</tr>
<tr>
<td>state</td>
<td>Activates debug printing of state transition on all PIM-SMv6 FSMs.</td>
</tr>
<tr>
<td>timer</td>
<td>Activates debug printing of PIM-SMv6 timers.</td>
</tr>
</tbody>
</table>

**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 28-1: 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
```
**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}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packet</td>
<td>Activates debug printing of incoming and/or outgoing IPv6 packets.</td>
</tr>
<tr>
<td>in</td>
<td>Specify incoming packet debugging.</td>
</tr>
<tr>
<td>out</td>
<td>Specify outgoing packet debugging.</td>
</tr>
</tbody>
</table>

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assert</td>
<td>Enable or disable debugging for the Assert timers.</td>
</tr>
<tr>
<td>at</td>
<td>Enable or disable debugging for the Assert Timer.</td>
</tr>
<tr>
<td>bsr</td>
<td>Enable or disable debugging for the specified Bootstrap Router timer, or all Bootstrap Router timers.</td>
</tr>
<tr>
<td>bst</td>
<td>Enable or disable debugging for the Bootstrap Router: Bootstrap Timer.</td>
</tr>
<tr>
<td>crp</td>
<td>Enable or disable debugging for the Bootstrap Router: Candidate-RP Timer.</td>
</tr>
<tr>
<td>hello</td>
<td>Enable or disable debugging for the specified Hello timer, or all Hello timers.</td>
</tr>
<tr>
<td>ht</td>
<td>Enable or disable debugging for the Hello timer: Hello Timer.</td>
</tr>
<tr>
<td>nlt</td>
<td>Enable or disable debugging for the Hello timer: Neighbor Liveness Timer.</td>
</tr>
<tr>
<td>tht</td>
<td>Enable or disable debugging for the Hello timer: Triggered Hello Timer.</td>
</tr>
<tr>
<td>joinprune</td>
<td>Enable or disable debugging for the specified JoinPrune timer, or all JoinPrune timers.</td>
</tr>
<tr>
<td>jt</td>
<td>Enable or disable debugging for the JoinPrune timer: upstream Join Timer.</td>
</tr>
<tr>
<td>et</td>
<td>Enable or disable debugging for the JoinPrune timer: Expiry Timer.</td>
</tr>
<tr>
<td>ppt</td>
<td>Enable or disable debugging for the JoinPrune timer: PrunePending Timer.</td>
</tr>
</tbody>
</table>
PIM-SMv6 COMMANDS
DEBUG IPV6 PIM SPARSE-MODE TIMER

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kat</td>
<td>Enable or disable debugging for the JoinPrune timer: KeepAlive Timer.</td>
</tr>
<tr>
<td>ot</td>
<td>Enable or disable debugging for the JoinPrune timer: Upstream Override Timer.</td>
</tr>
<tr>
<td>register</td>
<td>Enable or disable debugging for the Register timers.</td>
</tr>
<tr>
<td>rst</td>
<td>Enable or disable debugging for the Register timer: Register Stop Timer.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;access-list&gt;</code></td>
<td>Specify a Standard or an Extended software IPv6 Access list. See IPv6 Software Access Control List (ACL) Commands for supported IPv6 ACLs.</td>
</tr>
</tbody>
</table>

**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> ]

**Mode**  
Global Configuration

**Usage**  
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
```
PIM-SMV6 COMMANDS
IPV6 PIM BSR-CANDIDATE

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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>Specify the interface. For instance, VLAN interface vlan2.</td>
</tr>
<tr>
<td>&lt;hash&gt;</td>
<td>&lt;0-128&gt; configure the hash mask length used for RP selection. The default hash value if you do not configure this parameter is 126.</td>
</tr>
<tr>
<td>&lt;priority&gt;</td>
<td>&lt;0-255&gt; configure priority for a BSR candidate. Note that you must also specify the &lt;hash&gt; (mask length) when specifying the &lt;priority&gt;. The default priority if you do not configure this parameter is 64.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
terminal
configure
ipv6 forwarding
ipv6 multicast-routing
ipv6 pim bsr-candidate vlan2 20 30
```

To withdraw the address of vlan2 from being offered as a BSR candidate, enter:

```plaintext
terminal
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**
```plaintext
ipv6 pim cisco-register-checksum group-list <IPv6-access-list>
no ipv6 pim cisco-register-checksum group-list <IPv6-access-list>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPv6-access-list&gt;</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Default**
This command is disabled by default. By default, Register Checksum is calculated only over the header.

**Example**
```plaintext
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**
```
isv6 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
```

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interval&gt;</td>
<td>&lt;1-65535&gt; The value in seconds (no fractional seconds accepted).</td>
</tr>
</tbody>
</table>

**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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>Specifies the Join/Prune timer value. The default value is 210 seconds.</td>
</tr>
</tbody>
</table>

**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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPv6-accesslist&gt;</code></td>
<td>Specify a Standard or an Extended software IPv6 access list name for the PIM-SMv6 neighbor filter. See the <a href="#">IPv6 Software Access Control List (ACL) Commands</a> chapter for supported IPv6 ACLs.</td>
</tr>
</tbody>
</table>

**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:0ff: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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Specifies the maximum number of packets that can be sent per second.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-IPv6-address</td>
<td>The IPv6 address, entered in the form X:X::X:X, to be used as the source of the register packets.</td>
</tr>
<tr>
<td>interface</td>
<td>The name of the VLAN interface to be used as the source of the register packets.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Register suppression on time in seconds.</td>
</tr>
</tbody>
</table>

**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]
```

**Mode**
Global Configuration

**Usage**
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:10:5::153` will configure static-RP 3ffe:10:5::153 for the default group range ff00::/8. Configuring `ipv6 pim rp-address 3ffe: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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPv6-address&gt;</code></td>
<td>Specify the IPv6 address of the Rendezvous Point, entered in the form X:X::X:X.</td>
</tr>
<tr>
<td><code>&lt;IPv6-access-list&gt;</code></td>
<td>Specify a Standard or an Extended software IPv6 access-list name. See IPv6 Software Access Control List (ACL) Commands for supported IPv6 ACLs.</td>
</tr>
<tr>
<td>override</td>
<td>Specify this optional parameter keyword to enable any statically defined RPs to override dynamically learned RPs.</td>
</tr>
</tbody>
</table>
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

```plaintext
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 give the device the candidate RP (Rendezvous Point) status using the IPv6 address of the specified VLAN interface.

Use the `no` variant of this command to remove the RP status set using the `ipv6 pim rp-candidate` command.

**Syntax**

```
ipv6 pim rp-candidate <interface> [priority <priority>|interval <interval>| grouplist <accesslist>]
```

```
no ipv6 pim rp-candidate [<interface>]
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>Specify a VLAN interface name.</td>
</tr>
<tr>
<td><code>&lt;priority&gt;</code></td>
<td>&lt;0-255&gt; Specify this to configure the priority for an RP candidate.</td>
</tr>
<tr>
<td><code>&lt;interval&gt;</code></td>
<td>Specify a candidate RP advertisement interval in the range &lt;1-16383&gt; (seconds).</td>
</tr>
<tr>
<td><code>&lt;accesslist&gt;</code></td>
<td>Specify a Standard or an Extended software IPv6 access list name.</td>
</tr>
<tr>
<td></td>
<td>See the IPv6 Software Access Control List (ACL) Commands chapter for supported IPv6 ACLs.</td>
</tr>
</tbody>
</table>

**Default** The priority value for a candidate RP is 192 by default until specified using the `priority` parameter.

**Mode** Global Configuration

**Usage** 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**

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim rp-candidate vlan2 priority 3
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 priority 3
group-list G2
awplus# configure terminal
awplus(config)# no ipv6 pim rp-candidate vlan2
```
IPV6 PIM RP-CANDIDATE

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.

Note: 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
```

**Mode**
Global Configuration

**Default**
The default PIM-SMv6 KAT timer value is 210 seconds.

**Examples**

```
awplus# configure terminal
awplus(config)# ipv6 forward
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65536&gt;</td>
<td>Specify the KAT timer in seconds. The default value is 210 seconds.</td>
</tr>
</tbody>
</table>
**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(config-if)# 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.

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**
```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim spt-threshold
awplus# configure terminal
awplus(config)# no ipv6 pim spt-threshold
```
## 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 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>
```

### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPv6-access-list&gt;</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

### Mode
Global Configuration

### Examples
```
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
awplus# configure terminal
awplus(config)# no ipv6 pim spt-threshold group-list G1
```
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>]
nipv6 pim ssm
```

**Default**
By default, the command is disabled.

**Mode**
Global Configuration

**Usage**
Any (*,G) or (S,G,R) joins received for multicast groups (addresses) within the IPv6 address 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Named Standard Access List. Use FF3e::/32 group range for SSM.</td>
</tr>
<tr>
<td>range</td>
<td>Specify an ACL for group range to be used for SSM.</td>
</tr>
<tr>
<td>&lt;named-access-list&gt;</td>
<td>Specify a named standard access list.</td>
</tr>
</tbody>
</table>
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
show debugging ipv6 pim sparse-mode

Overview  This command displays the status of the PIM-SMv6 debugging on your device.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Syntax  show 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 28-2: Example output from the show debugging ipv6 pim sparse-mode command

```plaintext
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

unddebug 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 “Controlling “show” Command Output” in 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 28-3:  Example output from the show ipv6 pim sparse-mode bsr-router command

```plaintext
awplus#show ipv6 pim sparse-mode bsr-router
PIMv2 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 “Controlling “show” Command Output” in 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 VIF index Ver/Mode Nbr Count DR 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 28-1: Parameters in the output from the **show ipv6 pim sparse-mode interface** command

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Primary PIM-SMv6 address.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the PIM-SMv6 interface.</td>
</tr>
<tr>
<td>VIF Index</td>
<td>The Virtual Interface index of the VLAN.</td>
</tr>
<tr>
<td>Ver/Mode</td>
<td>PIMv6 version/Sparse mode.</td>
</tr>
<tr>
<td>Nbr Count</td>
<td>Neighbor count of the PIM-SMv6 interface.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>Designated Router priority.</td>
</tr>
<tr>
<td>DR</td>
<td>The IPv6 address of the Designated Router.</td>
</tr>
</tbody>
</table>
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 “Controlling “show” Command Output” in 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 28-4: 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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ipv6 pim sparse-mode local-members [interface]
```

**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 28-5: 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 28-6: 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
```
**PIM-SMV6 COMMANDS**

**SHOW IPV6 PIM SPARSE-MODE MRROUTE**

---

## 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 used simultaneously; two source IPv6 addresses cannot be used simultaneously.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

### Syntax

```
show ipv6 pim sparse-mode mroute
[<group-IPv6-address>|<source-IPv6-address>]
show ipv6 pim sparse-mode mroute [<group-IPv6-address>]
show ipv6 pim sparse-mode mroute [<source-IPv6-address>]
show ipv6 pim sparse-mode mroute [<source-IPv6-address>]
```

### Mode

User Exec and Privileged Exec

### Usage

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::
```
Figure 28-7: 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: 2
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 2

(*, ff0x::db8:0:0/96)
RP: 3ffe:10:10:5::153
RPF nbr: fe80::202:b3ff:fed4:69fe
RPF idx: wm0
Upstream State: JOINED
Local ...........................................
Joined ...........................................
Asserted ...........................................
FCR:
Source: 3ffe:10:10:1::96
Outgoing ...........................................
KAT timer running, 205 seconds remaining
Packet count 1

(*, ff0x::db8:0:0/96)
RP: 3ffe:10:10:5::153
RPF nbr: fe80::202:b3ff:fed4:69fe
RPF idx: wm0
Upstream State: JOINED
Local ...........................................
Joined ...........................................
Asserted ...........................................
FCR:
Source: 3ffe:10:10:1::96
Outgoing ...........................................
KAT timer running, 208 seconds remaining
Packet count 1
```
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 “Controlling “show” Command Output” in 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
```

**Usage**
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 28-8: Example output from the **show ipv6 pim sparse-mode mroute detail** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;group-IPv6-address&gt;</td>
<td>Group IPv6 address, entered in the form XX:XX. Output is all multicast entries belonging to that group.</td>
</tr>
<tr>
<td>&lt;source-IPv6-address&gt;</td>
<td>Source IPv6 address, entered in the form XX:XX. Output is all multicast entries belonging to that source.</td>
</tr>
<tr>
<td>detail</td>
<td>Show detailed information.</td>
</tr>
</tbody>
</table>
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: 4294967295l, Pref: 4294967295l, 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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show ipv6 pim sparse-mode neighbor [interface] [<IPv6-address>] [detail]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>Interface name (e.g. vlan2). Show neighbors on an interface.</td>
</tr>
<tr>
<td>&lt;IPv6-address&gt;</td>
<td>Show neighbors with a particular address on an interface. The IPv6 address</td>
</tr>
<tr>
<td></td>
<td>entered in the form X:X::X:X.</td>
</tr>
<tr>
<td>detail</td>
<td>Show detailed information.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Examples**
```
awplus# show ipv6 pim sparse-mode neighbor
awplus# show ipv6 pim sparse-mode neighbor vlan5 detail
```

Figure 28-9: 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 28-10: 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:10:10:3::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 “Controlling “show” Command Output” in 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 28-11: Example output from the show ipv6 pim sparse-mode nexthop command

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>Nexthop Num</th>
<th>Nexthop Addr</th>
<th>Nexthop IfIndex</th>
<th>Nexthop Metric</th>
<th>Pref</th>
<th>Refcnt</th>
</tr>
</thead>
<tbody>
<tr>
<td>3ffe:10:10:5::153</td>
<td>.RS.</td>
<td>1</td>
<td>fe80::20e:cf:e01:facc</td>
<td>2</td>
<td>30</td>
<td>110</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 28-2: Parameters in output of the show ipv6 pim sparse-mode nexthop command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The destination address for which PIM-SMv6 requires next hop information.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of destination, as indicated by the Flags description. N = New, R = RP, S = Source, U = Unreachable.</td>
</tr>
<tr>
<td>Nexthop Num</td>
<td>The number of next hops to the destination. PIM-SMv6 always uses only 1 next hop.</td>
</tr>
<tr>
<td>Nexthop Addr</td>
<td>The address of the primary next hop gateway.</td>
</tr>
<tr>
<td>Nexthop IfIndex</td>
<td>The interface on which the next hop gateway can be reached.</td>
</tr>
<tr>
<td>Nexthop Name</td>
<td>The name of next hop interface.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric of the route towards the destination.</td>
</tr>
<tr>
<td>Preference</td>
<td>The preference of the route towards destination.</td>
</tr>
<tr>
<td>Refcnt</td>
<td>Only used for debugging.</td>
</tr>
</tbody>
</table>
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**

```
show ipv6 pim sparse-mode rp-hash <IPv6-group-addr>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPv6-group-addr&gt;</td>
<td>The IPv6 group address used to find the RP, entered in the form X::X::X.</td>
</tr>
</tbody>
</table>

**Mode**

User Exec and Privileged Exec

**Example**

```
awplus# show ipv6 pim sparse-mode rp-hash ff04:10
```

Figure 28-12: Output from the `show ipv6 pim sparse-mode rp-hash` command:

```
awplus# show ipv6 pim sparse-mode rp-hash ff04::10
  RP: 3ffe:10:5:5::153
  Info source: 3ffe:10:5:5::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 “Controlling “show” Command Output” in 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 28-13: 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 “Controlling “show” Command Output” in 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 XX::XX.

**Mode**
User Exec and Privileged Exec

**Example**
```
awplus# show ipv6 pim sparse-mode rp nexthop 3ffe:10:10:5::153
```

Figure 28-14: Example output from the `show ipv6 pim sparse-mode rp nexthop` command

```plaintext
awplus# show ipv6 pim sparse-mode rp nexthop 3ffe:10:10:5::153
Flags: N = New, R = RP, S = Source, U = Unreachable

Destination | Type | Nexthop Num | Nexthop Addr | Nexthop IfIndex | Nexthop Name
--- | --- | --- | --- | --- | ---
3ffe:10:10:5::153 | .RS. | 1 | fe80::20e:cff:fe01:facc | 2 | 30 | 110 | 1
```

Table 28-3: 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 28-3: Parameters in output of the `show ipv6 pim sparse-mode rp nexthop` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric</td>
<td>The metric of the route towards the destination.</td>
</tr>
<tr>
<td>Preference</td>
<td>The preference of the route towards destination.</td>
</tr>
<tr>
<td>Refcnt</td>
<td>Only used for debugging.</td>
</tr>
</tbody>
</table>
**undebug all ipv6 pim sparse-mode**

**Overview**
Use this command to disable all PIM-SMv6 debugging.

**Syntax**
```plaintext
undebug all ipv6 pim sparse-mode
```

**Mode**
Privileged Exec

**Example**
```plaintext
awplus# undebug all ipv6 pim sparse-mode
```

**Related commands**
`debug ipv6 pim sparse-mode`
**PIM-SMV6 COMMANDS**

**UNDEBUG 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Deactivates all PIM-SMv6 debugging.</td>
</tr>
<tr>
<td>events</td>
<td>Deactivates debug printing of PIM-SMv6 events.</td>
</tr>
<tr>
<td>mfc</td>
<td>Deactivates debug printing of MFC (Multicast Forwarding Cache).</td>
</tr>
<tr>
<td>mib</td>
<td>Deactivates debug printing of PIM-SMv6 MIBs.</td>
</tr>
<tr>
<td>nexthop</td>
<td>Deactivates debug printing of PIM-SMv6 next hop communications.</td>
</tr>
<tr>
<td>nsm</td>
<td>Deactivates debugging of PIM-SMv6 NSM (Network Services Module) communications.</td>
</tr>
<tr>
<td>state</td>
<td>Deactivates debug printing of state transition on all PIM-SMv6 FSMs.</td>
</tr>
<tr>
<td>timer</td>
<td>Deactivates debug printing of PIM-SMv6 timers.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec and Global Configuration

**Example**
```
aplus# configure terminal
aplus(config)# terminal monitor
aplus(config)# undebug ipv6 pim sparse-mode all
aplus# configure terminal
aplus(config)# terminal monitor
aplus(config)# undebug ipv6 pim sparse-mode events
aplus# configure terminal
aplus(config)# terminal monitor
aplus(config)# undebug ipv6 pim sparse-mode nexthop
```
**Validation Output**

Figure 28-15: 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`
29 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.
PIM-DM COMMANDS

Command List

- “debug pim dense-mode all” on page 1268
- “debug pim dense-mode context” on page 1269
- “debug pim dense-mode decode” on page 1270
- “debug pim dense-mode encode” on page 1271
- “debug pim dense-mode fsm” on page 1272
- “debug pim dense-mode mrt” on page 1273
- “debug pim dense-mode nexthop” on page 1274
- “debug pim dense-mode nsm” on page 1275
- “debug pim dense-mode vif” on page 1276
- “ip pim dense-mode” on page 1277
- “ip pim dense-mode passive” on page 1278
- “ip pim ext-srscs-directly-connected (PIM-DM)” on page 1279
- “ip pim hello-holdtime (PIM-DM)” on page 1280
- “ip pim hello-interval (PIM-DM)” on page 1281
- “ip pim max-graft-retries” on page 1282
- “ip pim neighbor-filter (PIM-DM)” on page 1284
- “ip pim propagation-delay” on page 1285
- “ip pim state-refresh origination-interval” on page 1286
- “show debugging pim dense-mode” on page 1287
- “show ip pim dense-mode interface” on page 1288
- “show ip pim dense-mode interface detail” on page 1290
- “show ip pim dense-mode mroute” on page 1291
- “show ip pim dense-mode neighbor” on page 1292
- “show ip pim dense-mode neighbor detail” on page 1293
- “show ip pim dense-mode nexthop” on page 1294
- “undebug all pim dense-mode” on page 1295
### 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 29-1: 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
depug pim dense-mode all
depug pim dense-mode context
depug pim dense-mode encode
depug pim dense-mode fsm
depug pim dense-mode mrt
depug pim dense-mode nexthop
depug pim dense-mode nsm
depug 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**
d debug pim dense-mode all
d debug pim dense-mode context
d debug pim dense-mode decode
d debug pim dense-mode encode
d debug pim dense-mode mrt
d debug pim dense-mode nexthop
d debug pim dense-mode nsm
d 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**
d 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**
d debug pim dense-mode all
d debug pim dense-mode context
d debug pim dense-mode decode
d debug pim dense-mode encode
d debug pim dense-mode fsm
d debug pim dense-mode mrt
d debug pim dense-mode nsm
d 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**
depug 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**
depug pim dense-mode all
depug pim dense-mode context
depug pim dense-mode decode
depug pim dense-mode encode
depug pim dense-mode fsm
depug pim dense-mode mrt
depug pim dense-mode nexthop
depug 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 ext-srcs-directly-connected (PIM-DM)

**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.

This command is described in detail in the PIM-SM Commands chapter. See the ip pim ext-srcs-directly-connected (PIM-SM) command.
**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).

**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**

```plaintext
ip pim hello-interval <interval>
no ip pim hello-interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interval&gt;</td>
<td>&lt;1-65535&gt; The value in seconds (no fractional seconds accepted).</td>
</tr>
</tbody>
</table>

**Mode**  Interface Configuration for a VLAN interface.

**Example**

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip pim hello-interval 123
```
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Negate a command or set its defaults.</td>
</tr>
<tr>
<td>ip</td>
<td>Internet Protocol (IP).</td>
</tr>
<tr>
<td>pim</td>
<td>PIM Interface commands.</td>
</tr>
<tr>
<td>max-graft-retries</td>
<td>PIM Graft message retries.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Graft message retries before ceasing Graft message retries.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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`
**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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;number&gt;</td>
<td>&lt;1-99&gt; Standard IP access list number.</td>
</tr>
<tr>
<td>&lt;accesslist&gt;</td>
<td>IP access list name.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;delay&gt;</td>
<td>&lt;1000-5000&gt; The value in milliseconds. The default is 1000 milliseconds.</td>
</tr>
</tbody>
</table>

**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
```
**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
```

**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
```
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 “Controlling “show” Command Output” in 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 29-2: 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 VIP 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 “Controlling “show” Command Output” in 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/Mode Nbr 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 29-1: Parameters in the output of the **show ip pim dense-mode interface** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total configured interfaces</td>
<td>The number of configured PIM Dense Mode interfaces.</td>
</tr>
<tr>
<td>Maximum allowed</td>
<td>The maximum number of PIM Dense Mode interfaces that can be configured.</td>
</tr>
<tr>
<td>Total active interfaces</td>
<td>The number of active PIM Dense Mode interfaces.</td>
</tr>
<tr>
<td>Address</td>
<td>Primary PIM-DM address.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the PIM-DM interface.</td>
</tr>
<tr>
<td>VIF Index</td>
<td>The Virtual Interface index of the VLAN.</td>
</tr>
<tr>
<td>Ver/Mode</td>
<td>PIM version/Dense mode.</td>
</tr>
<tr>
<td>Nbr Count</td>
<td>Neighbor count of the PIM-DM interface.</td>
</tr>
</tbody>
</table>
PIM-DM COMMANDS
SHOW IP PIM DENSE-MODE 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 “Controlling “show” Command Output” in 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 29-3: Example output from the `show ip pim dense-mode interface detail` command

```plaintext
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 “Controlling “show” Command Output” in 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 29-4: 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 “Controlling “show” Command Output” in 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**  
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 29-5:  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 “Controlling “show”
Command Output” in 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 29-6: 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 “Controlling “show” Command Output” in 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 29-7: Example output from the show ip pim dense-mode neighbor nexthop command

<table>
<thead>
<tr>
<th>Destination</th>
<th>Nexthop Num</th>
<th>Nexthop Addr</th>
<th>Nexthop Interface</th>
<th>Metric</th>
<th>Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.52</td>
<td>1</td>
<td>0.0.0.0</td>
<td>vlan2</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 29-2: Parameters in the output of the show ip pim dense-mode neighbor nexthop command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Destination address for which PIM-DM requires next hop information.</td>
</tr>
<tr>
<td>Nexthop Num</td>
<td>Number of next hops to the destination. PIM can only use one next hop.</td>
</tr>
<tr>
<td>Nexthop Addr</td>
<td>Address of the current next hop gateway.</td>
</tr>
<tr>
<td>Nexthop Interface</td>
<td>Name of the next hop interface.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric of the route towards the destination.</td>
</tr>
<tr>
<td>Preference</td>
<td>Preference of the route towards the destination.</td>
</tr>
</tbody>
</table>
**PIM-DM COMMANDS**
**UNDEBUG ALL PIM DENSE-MODE**

---

### 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**
d debug pim dense-mode all
d debug pim dense-mode context
d debug pim dense-mode decode
d debug pim dense-mode encode
d debug pim dense-mode fsm
d debug pim dense-mode mrt
d debug pim dense-mode nexthop
d debug pim dense-mode nsm
d debug pim dense-mode vif
Introduction

Overview  This chapter provides an alphabetical reference of IPv4 Hardware Access Control List (ACL) commands. It contains detailed command information and command examples about IPv4 hardware ACLs, which are applied directly to interfaces using the access-group command.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself.

• Text in parenthesis in command names indicates usage not keyword entry. For example, access-list hardware (named) indicates named IPv4 hardware ACLs entered as access-list hardware <name> where <name> is a placeholder not a keyword.

• Parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as (access-list standard numbered filter) represents command entry in the format shown in the syntax [<sequence-number>] {deny|permit} {<source>|host <host-address>|any}.

• Software ACLs will deny access unless explicitly permitted by an ACL action.

Sub-modes  Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 30-1: IPv4 Hardware Access List Commands and Prompts

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Command Mode</th>
<th>Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface access-group</td>
<td>Privileged Exec</td>
<td>awplus#</td>
</tr>
<tr>
<td>show access-list (IPv4 Hardware ACLs)</td>
<td>Privileged Exec</td>
<td>awplus#</td>
</tr>
<tr>
<td>show interface access-group</td>
<td>Privileged Exec</td>
<td>awplus#</td>
</tr>
</tbody>
</table>
### 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 1297
- “access-list (hardware IP numbered)” on page 1299
- “access-list (hardware MAC numbered)” on page 1309
- “access-list hardware (named)” on page 1312
- “(access-list hardware ICMP filter)” on page 1314
- “(access-list hardware IP protocol filter)” on page 1317
- “(access-list hardware MAC filter)” on page 1323
- “(access-list hardware TCP UDP filter)” on page 1326
- “commit (IPv4)” on page 1329
- “show access-list (IPv4 Hardware ACLs)” on page 1330
- “show interface access-group” on page 1332

---

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Command Mode</th>
<th>Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-group</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>access-list (hardware IP numbered)</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>access-list (hardware MAC numbered)</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>access-list hardware (named)</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>access-group</td>
<td>Interface Configuration</td>
<td>awplus(config-if)#</td>
</tr>
<tr>
<td>(access-list hardware ICMP filter)</td>
<td>IPv4 Hardware ACL</td>
<td>awplus(config-ip-hw-acl)#</td>
</tr>
<tr>
<td>(access-list hardware IP protocol filter)</td>
<td>IPv4 Hardware ACL</td>
<td>awplus(config-ip-hw-acl)#</td>
</tr>
<tr>
<td>(access-list hardware MAC filter)</td>
<td>IPv4 Hardware ACL</td>
<td>awplus(config-ip-hw-acl)#</td>
</tr>
<tr>
<td>(access-list hardware TCP UDP filter)</td>
<td>IPv4 Hardware ACL</td>
<td>awplus(config-ip-hw-acl)#</td>
</tr>
<tr>
<td>commit (IPv4)</td>
<td>IPv4 Hardware ACL</td>
<td>awplus(config-ip-hw-acl)#</td>
</tr>
</tbody>
</table>
access-group

**Overview**  
This command adds or removes a hardware-based access-list to or from a switch port interface. The number of hardware numbered and named access-lists that can be added to a switch port interface is determined by the available memory in hardware-based packet classification tables.

This command works in Interface Configuration mode to apply hardware access-lists to selected switch port interfaces.

The **no** variant of this command removes the selected access-list from an interface.

**Syntax**
```plaintext
access-group
[<3000-3699>|<4000-4699>|<hardware-access-list-name>]

no access-group
[<3000-3699>|4000-4699|<hardware-access-list-name>]
```

**Parameter** | **Description**
--- | ---
<3000-3699> | Hardware IP access-list.
<4000-4699> | Hardware MAC access-list.
<hardware-access-list-name> | The hardware access-list name.

**Mode**  
Interface Configuration for a switch port interface

**Default**  
Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage**  
First create an IP access-list that applies the appropriate permit/deny requirements with the `access-list (hardware IP numbered)` command, the `access-list (hardware MAC numbered)` command or the `access-list hardware (named)` command. Then use this command to apply this hardware access-list to a specific port or port range. Note that this command will apply the access-list only to incoming data packets.

To apply ACLs to an LACP aggregated link, apply it to all the individual switch ports in the aggregated group. To apply ACLs to a static channel group, apply it to the static channel group itself. An ACL can even be applied to a static aggregated link that spans more than one switch instance (Link Aggregation Commands).

Note that you cannot apply software numbered ACLs to switch port interfaces with the access-group command. This command will only apply hardware ACLs.

**NOTE:** Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Examples**  
To add the numbered hardware access-list 3005 to switch port interface port1.0.1, enter the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# access-group 3005
```
To add the named hardware access-list `hw-acl` to switch port interface `port1.0.2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# access-group hw-acl
```

To apply an ACL to static channel group 2 containing switch port `port1.0.5` and `port1.0.6`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5-1.0.6
awplus(config-if)# static-channel-group 2
awplus(config)# interface sa2
awplus(config-if)# access-group 3000
```
access-list (hardware IP numbered)

**Overview**  This command creates an access-list for use with hardware classification, such as QoS. The access-list will match on either TCP or UDP type packets that have the specified source and destination IP addresses and Layer 4 port values or ranges. The parameter **any** may be specified if an address does not matter and the port values are optional.

The no variant of this command removes the previously specified IP hardware access-list.

**Syntax [ip]**
```
access-list <3000-3699>
{deny|permit|copy-to-cpu|copy-to-mirror|send-to-mirror|send-to-cpu} ip <source> <destination>
```

**Syntax [icmp]**
```
access-list <3000-3699>
{deny|permit|copy-to-cpu|copy-to-mirror|send-to-mirror|send-to-cpu} icmp <source> <destination> [icmp-type <type-number>]
```

```
no access-list <3000-3699>
```

**Table 30-2: Parameters in the access-list (hardware IP numbered) command - ip|icmp**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;3000-3699&gt;</td>
<td>Hardware IP access-list number.</td>
</tr>
<tr>
<td>deny</td>
<td>Access-list rejects packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>Access-list permits packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>copy-to-cpu</td>
<td>Specify packets to copy to the CPU.</td>
</tr>
<tr>
<td>copy-to-mirror</td>
<td>Specify packets to copy to the mirror port.</td>
</tr>
<tr>
<td>send-to-mirror</td>
<td>Specify packets to send to the mirror port.</td>
</tr>
<tr>
<td>send-to-cpu</td>
<td>Specify packets to send to the CPU.</td>
</tr>
<tr>
<td>icmp</td>
<td>ICMP packet.</td>
</tr>
<tr>
<td>ip</td>
<td>IP packet.</td>
</tr>
</tbody>
</table>
### Parameters in the access-list (hardware IP numbered) command - ip|icmp (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;source&gt;</code></td>
<td>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:</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single source host with the IP address given by <code>&lt;ip-addr&gt;</code> in dotted decimal notation.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;/prefix</code></td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;reverse-mask</code></td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
<tr>
<td><code>&lt;destination&gt;</code></td>
<td>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:</td>
</tr>
<tr>
<td>any</td>
<td>Matches any destination IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single destination host with the IP address given by <code>&lt;ip-addr&gt;</code> in dotted decimal notation.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;/prefix</code></td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;reverse-mask</code></td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
<tr>
<td>icmp-type</td>
<td>Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets.</td>
</tr>
</tbody>
</table>
Table 30-2: **Parameters in the access-list (hardware IP numbered) command - ip|icmp (cont.)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;type-number&gt;</td>
<td>The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type:</td>
</tr>
<tr>
<td>0</td>
<td>Echo replies.</td>
</tr>
<tr>
<td>3</td>
<td>Destination unreachable messages.</td>
</tr>
<tr>
<td>4</td>
<td>Source quench messages.</td>
</tr>
<tr>
<td>5</td>
<td>Redirect (change route) messages.</td>
</tr>
<tr>
<td>8</td>
<td>Echo requests.</td>
</tr>
<tr>
<td>11</td>
<td>Time exceeded messages.</td>
</tr>
<tr>
<td>12</td>
<td>Parameter problem messages.</td>
</tr>
<tr>
<td>13</td>
<td>Timestamp requests.</td>
</tr>
<tr>
<td>14</td>
<td>Timestamp replies.</td>
</tr>
<tr>
<td>15</td>
<td>Information requests.</td>
</tr>
<tr>
<td>16</td>
<td>Information replies.</td>
</tr>
<tr>
<td>17</td>
<td>Address mask requests.</td>
</tr>
<tr>
<td>18</td>
<td>Address mask replies.</td>
</tr>
</tbody>
</table>

**Syntax [tcp|udp]**

```
access-list <3000-3699>
{copy-to-cpu|copy-to-mirror|send-to-mirror|deny|permit|send-to-cpu} {tcp|udp} <source> {eq <sourceport>|lt <sourceport>|gt <sourceport>|ne <sourceport>| [range <start-range> <end-range>] <destination> {eq <destport>|lt <destport>|gt <destport>|ne <destport>| [range <start-range> <end-range>]}
no access-list <3000-3699>
```

Table 30-3: **Parameters in the access-list (hardware IP numbered) command - tcp|udp**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;3000-3699&gt;</td>
<td>Hardware IP access-list.</td>
</tr>
<tr>
<td>copy-to-cpu</td>
<td>Specify packets to copy to the CPU.</td>
</tr>
<tr>
<td>copy-to-mirror</td>
<td>Specify packets to copy to the mirror port.</td>
</tr>
<tr>
<td>send-to-mirror</td>
<td>Specify packets to send to the mirror port.</td>
</tr>
<tr>
<td>deny</td>
<td>The access-list rejects packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>The access-list permits packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td>send-to-cpu</td>
<td>Specify packets to send to the CPU.</td>
</tr>
</tbody>
</table>
## IPV4 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS

### access-list (hardware IP numbered)

#### Table 30-3: **Parameters in the access-list (hardware IP numbered) command - tcp|udp (cont.)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>The access-list matches only TCP packets.</td>
</tr>
<tr>
<td>udp</td>
<td>The access-list matches only UDP packets.</td>
</tr>
<tr>
<td>&lt;source&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single source host with the IP address given by &lt;ip-addr&gt; in dotted decimal notation.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;/&lt;prefix&gt;</td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
<tr>
<td>&lt;destination&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>any</td>
<td>Matches any destination IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single destination host with the IP address given by &lt;ip-addr&gt; in dotted decimal notation.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;/&lt;prefix&gt;</td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
<tr>
<td>&lt;sourceport&gt;</td>
<td>The source (TCP or UDP) port number, specified as an integer between 0 and 65535.</td>
</tr>
<tr>
<td>range</td>
<td>Range of port numbers.</td>
</tr>
</tbody>
</table>
### Parameters in the access-list (hardware IP numbered) command - tcp|udp (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;start-range&gt;</code></td>
<td>Port number at start of range <code>&lt;0-65535&gt;</code></td>
</tr>
<tr>
<td><code>&lt;end-range&gt;</code></td>
<td>Port number at end of range <code>&lt;0-65535&gt;</code></td>
</tr>
<tr>
<td><code>&lt;destport&gt;</code></td>
<td>The destination (TCP or UDP) port number, specified as an integer between 0 and 65535.</td>
</tr>
<tr>
<td><code>eq</code></td>
<td>Matches port numbers that are equal to the port number specified immediately after this parameter.</td>
</tr>
<tr>
<td><code>lt</code></td>
<td>Matches port numbers that are less than the port number specified immediately after this parameter.</td>
</tr>
<tr>
<td><code>gt</code></td>
<td>Matches port numbers that are greater than the port number specified immediately after this parameter.</td>
</tr>
<tr>
<td><code>ne</code></td>
<td>Matches port numbers that are not equal to the port number specified immediately after this parameter.</td>
</tr>
</tbody>
</table>

### Syntax [proto]

```
access-list <3000-3699>
{copy-to-cpu|copy-to-mirror|send-to-mirror|deny|permit|send-to-cpu} proto <ip-protocol> <source> <destination>
```

```
no access-list <3000-3699>
```

### Parameters in the access-list (hardware IP numbered) command - proto

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;3000-3699&gt;</code></td>
<td>Hardware IP access-list.</td>
</tr>
<tr>
<td><code>copy-to-cpu</code></td>
<td>Specify packets to copy to the CPU.</td>
</tr>
<tr>
<td><code>copy-to-mirror</code></td>
<td>Specify packets to copy to the mirror port.</td>
</tr>
<tr>
<td><code>send-to-mirror</code></td>
<td>Specify packets to send to the mirror port</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>Access-list rejects packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Access-list permits packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td><code>send-to-cpu</code></td>
<td>Specify packets to send to the CPU.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&lt;source&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single source host with the IP address given by &lt;ip-addr&gt; in dotted decimal notation.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;/&lt;prefix&gt;</td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;/&lt;reverse-mask&gt;</td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
<tr>
<td>&lt;destination&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>any</td>
<td>Matches any destination IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single destination host with the IP address given by &lt;ip-addr&gt; in dotted decimal notation.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;/&lt;prefix&gt;</td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;/&lt;reverse-mask&gt;</td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
<tr>
<td>proto</td>
<td>Matches only a specified type of IP Protocol &lt;1-255&gt;.</td>
</tr>
</tbody>
</table>
Table 30-4: Parameters in the `access-list (hardware IP numbered)` command - proto (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-protocol&gt;</code></td>
<td>The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority [<a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a>])</td>
</tr>
<tr>
<td>Protocol Number</td>
<td>Protocol Description [RFC Reference]</td>
</tr>
<tr>
<td>1</td>
<td>Internet Control Message [RFC792]</td>
</tr>
<tr>
<td>2</td>
<td>Internet Group Management [RFC1112]</td>
</tr>
<tr>
<td>3</td>
<td>Gateway-to-Gateway [RFC823]</td>
</tr>
<tr>
<td>4</td>
<td>IP in IP [RFC2003]</td>
</tr>
<tr>
<td>5</td>
<td>Stream [RFC1190] [RFC1819]</td>
</tr>
<tr>
<td>6</td>
<td>TCP (Transmission Control Protocol) [RFC793]</td>
</tr>
<tr>
<td>8</td>
<td>EGP (Exterior Gateway Protocol) [RFC888]</td>
</tr>
<tr>
<td>9</td>
<td>IGP (Interior Gateway Protocol) [IANA]</td>
</tr>
<tr>
<td>11</td>
<td>Network Voice Protocol [RFC741]</td>
</tr>
<tr>
<td>17</td>
<td>UDP (User Datagram Protocol) [RFC768]</td>
</tr>
<tr>
<td>20</td>
<td>Host monitoring [RFC869]</td>
</tr>
<tr>
<td>27</td>
<td>RDP (Reliable Data Protocol) [RFC908]</td>
</tr>
<tr>
<td>28</td>
<td>IRTP (Internet Reliable Transaction Protocol) [RFC938]</td>
</tr>
<tr>
<td>29</td>
<td>ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]</td>
</tr>
</tbody>
</table>
IPV4 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS
ACCESS-LIST (HARDWARE IP NUMBERED)

Table 30-4: Parameters in the access-list (hardware IP numbered) command - proto (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-protocol&gt; (cont.)</td>
<td>Bulk Data Transfer Protocol [RFC969]</td>
</tr>
<tr>
<td>30</td>
<td>DCCP (Datagram Congestion Control Protocol) [RFC4340]</td>
</tr>
<tr>
<td>33</td>
<td>DSR (Dynamic Source Routing Protocol) [RFC4728]</td>
</tr>
<tr>
<td>48</td>
<td>ESP (Encap Security Payload) [RFC2406]</td>
</tr>
<tr>
<td>50</td>
<td>AH (Authentication Header) [RFC2402]</td>
</tr>
<tr>
<td>51</td>
<td>NARP (NBMA Address Resolution Protocol) [RFC1735]</td>
</tr>
<tr>
<td>54</td>
<td>EIGRP (Enhanced Interior Gateway Routing Protocol)</td>
</tr>
<tr>
<td>88</td>
<td>OSPF/IGP [RFC1583]</td>
</tr>
<tr>
<td>89</td>
<td>Ethernet-within-IP Encapsulation / RFC3378</td>
</tr>
<tr>
<td>97</td>
<td>Encapsulation Header / RFC1241</td>
</tr>
<tr>
<td>98</td>
<td>IP Payload Compression Protocol / RFC2393</td>
</tr>
<tr>
<td>108</td>
<td>Virtual Router Redundancy Protocol / RFC3768</td>
</tr>
<tr>
<td>112</td>
<td>RSVP-E2E-IGNORE / RFC3175</td>
</tr>
<tr>
<td>134</td>
<td>Mobility Header / RFC3775</td>
</tr>
<tr>
<td>135</td>
<td>UDPLite / RFC3828</td>
</tr>
<tr>
<td>136</td>
<td>MPLS-in-IP / RFC4023</td>
</tr>
<tr>
<td>137</td>
<td>MANET Protocols / RFC-ietf-manet-iana-07.txt</td>
</tr>
<tr>
<td>138</td>
<td>Unassigned / IANA</td>
</tr>
<tr>
<td>139-252</td>
<td>Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td>253</td>
<td>Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td>254</td>
<td>Reserved / IANA</td>
</tr>
<tr>
<td>255</td>
<td></td>
</tr>
</tbody>
</table>

Mode  Global Configuration

Default  Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.
**Usage**

This command creates an access-list for use with hardware classification, such as when applying QoS. This command can be used to match ICMP packets, IP protocols, or TCP/UDP packets.

For ICMP packets, the `<3000-3699>` range IP hardware access-list will match any ICMP packet that has the specified source and destination IP addresses and ICMP type.

You may apply the `any` parameter if the source or destination IP address is not important. The ICMP type is an optional parameter.

*NOTE:* Hardware ACLs will *permit* access unless *explicitly denied* by an ACL action.

**Examples**

Follow the below example commands to configure access-lists for ICMP, IP protocol and TCP.

**ICMP Example**

To create an access-list that will permit ICMP packets with a source address of 192.168.1.0/24 with any destination address and an ICMP type of 5 enter the below commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit icmp 192.168.1.0/24 any icmp-type 5
```

To destroy the access-list with an access-list identity of 3000 enter the below commands:

```
awplus# configure terminal
awplus(config)# no access-list 3000
```

**IP Example**

To create an access-list that will permit any type of IP packet with a source address of 192.168.1.1 and any destination address, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit ip 192.168.1.1/32 any
```

To create an access-list that will deny all IGMP packets (IP protocol 2) from the 192.168.0.0 network, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 deny proto 2 192.168.0.0/16 any
```

**TCP Example**

To create an access-list that will permit TCP packets with a destination address of 192.168.1.1, a destination port of 80 and any source address and source port, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit tcp any 192.168.1.1/32 eq 80
```
**copy-to-mirror Example**

To create an access-list that will copy-to-mirror TCP packets with a destination address of 192.168.1.1, a destination port of 80 and any source address and source port for use with the mirror interface command, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 copy-to-mirror tcp any 192.168.1.1/32 eq 80
```

**Related Commands**

- access-group
- mirror interface
- show running-config
- show access-list (IPv4 Hardware ACLs)
access-list (hardware MAC numbered)

**Overview** This command creates an access-list for use with hardware classification, such as QOS. The access-list will match on packets that have the specified source and destination MAC addresses. The parameter `any` may be specified if an address does not matter.

The `no` variant of this command removes the specified MAC hardware filter access-list.

**Syntax**

```
access-list <4000-4699> 
{copy-to-cpu|copy-to-mirror|deny|permit|send-to-cpu} 
{<source-mac-address>|any}{<destination-mac-address>|any}
```

```
no access-list <4000-4699>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;4000-4699&gt;</code></td>
<td>Hardware MAC access-list.</td>
</tr>
<tr>
<td><code>copy-to-cpu</code></td>
<td>Specify packets to copy to the CPU.</td>
</tr>
<tr>
<td><code>copy-to-mirror</code></td>
<td>Specify packets to copy to the mirror port.</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>Access-list rejects packets that match the source and destination filtering.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Access-list permits packets that match the source and destination filtering.</td>
</tr>
<tr>
<td><code>send-to-cpu</code></td>
<td>Specify packets to send to the CPU.</td>
</tr>
<tr>
<td><code>&lt;source-mac-address&gt;</code></td>
<td>The source MAC address of the packets. Enter this in the format <code>&lt;HHHH.HHHH.HHHH&gt;</code> where each <code>H</code> is a hexadecimal number that represents a 4 bit binary number.</td>
</tr>
<tr>
<td><code>&lt;source-mac-mask&gt;</code></td>
<td>The mask that will be applied to the source MAC addresses. Enter this in the format <code>&lt;HHHH.HHHH.HHHH&gt;</code> where each <code>H</code> is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either 0 or F. Where Hex FF = Ignore, and Hex 00 = Match.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Any source MAC address.</td>
</tr>
<tr>
<td><code>&lt;destination-mac-address&gt;</code></td>
<td>The destination MAC address of the packets. Enter this in the format <code>&lt;HHHH.HHHH.HHHH&gt;</code> where each <code>H</code> is a hexadecimal number that represents a 4 bit binary number.</td>
</tr>
</tbody>
</table>
IPV4 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS
access-list (hardware MAC numbered)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;destination-mac-mask&gt;</td>
<td>The mask that will be applied to the destination MAC addresses. Enter this in the format &lt;HHHH.HHHH.HHHH&gt; where each H is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either 0 or F. Where Hex FF = Ignore, and Hex 00 = Match.</td>
</tr>
<tr>
<td>any</td>
<td>Any destination MAC address.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specifies that the ACL will match on the ID in the packet’s VLAN tag.</td>
</tr>
<tr>
<td>&lt;1-4094&gt;</td>
<td>The VLAN VID.</td>
</tr>
<tr>
<td>inner-vlan</td>
<td>This parameter is used within double-tagged VLANs. It is the inner VLAN tag (VID); sometimes referred to as the C-TAG (Customer VLAN TAG), where the vlan VID tag is referred to as the S-TAG (Service VLAN TAG).</td>
</tr>
<tr>
<td>&lt;1-4094&gt;</td>
<td>The inner VLAN VID.</td>
</tr>
</tbody>
</table>

**Mode**  
Global Configuration

**Default**  
Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage**  
This command creates an access-list for use with hardware classification, such as when applying QoS. The <4000-4699> range MAC hardware access-list will match on packets that have the specified source and destination MAC addresses. You may apply the any parameter if the source or destination MAC host address is not important.

**NOTE:** Hardware ACLs will permit access unless explicitly denied by an ACL action.

**Examples**  
To create an access-list that will permit packets with a MAC address of 0000.00ab.1234 and any destination address enter the commands:

```plaintext
awplus# configure terminal
awplus(config)# access-list 4000 permit 0000.00ab.1234 0000.0000.0000 any
```

To create an access-list that will permit packets with an initial MAC address component of 0000.00ab and any destination address, enter the commands:

```plaintext
awplus# configure terminal
awplus(config)# access-list 4001 permit 0000.00ab.1234 0000.0000.FFFF any
```
To create an access-list that will copy-to-mirror packets with an initial MAC address component of 0000.00ab and any destination address for use with the `mirror interface` command, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 copy-to-mirror 0000.00ab.1234 0000.0000.FFFF any
```

To destroy the access-list with an access-list identity of 4000 enter the commands:

```
awplus# configure terminal
awplus(config)# no access-list 4000
```

**Related Commands**

- `access-group`
- `mirror interface`
- `show running-config`
- `show access-list (IPv4 Hardware ACLs)`
access-list hardware (named)

**Overview**
This command creates a named hardware access-list that can be applied to a switch port interface. ACL filters for a named hardware ACL are created in the IPv4 Hardware ACL Configuration mode.

The `no` variant of this command removes the specified named hardware ACL.

**Syntax**

```
access-list hardware <hardware-access-list-name>
no access-list hardware <hardware-access-list-name>
```

**Parameter**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;hardware-access-list-name&gt;</code> Specify the hardware ACL name to then define ACL filters for in the subsequent IPv4 Hardware ACL Configuration mode.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Default**
Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage**
Use this command to name a hardware ACL and enter the IPv4 Hardware ACL Configuration mode. If the named hardware ACL doesn't exist, it will be created after entry. If the named hardware ACL does exist, then you can enter IPv4 Hardware ACL Configuration mode for that existing ACL.

Entering this command with the hardware ACL name moves you to the (config-ip-hw-acl) prompt for the IPv4 Hardware ACL Configuration mode so you can enter ACL filters with sequence numbers. From this prompt, configure the filters for the ACL. See the [ACL Feature Overview and Configuration Guide](#) for complete examples of configured sequenced numbered ACLs.

**NOTE:** Hardware ACLs will permit access unless explicitly denied by an ACL action.

**Examples**
To create the hardware access-list named `ACL-1` and enter the IPv4 Hardware ACL Configuration mode to specify the ACL filter entry, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware ACL-1
awplus(config-ip-hw-acl)#
```

To remove the hardware access-list named `ACL-1`, use the commands:

```
awplus# configure terminal
awplus(config)# no access-list hardware ACL-1
```
**Related Commands**

- `access-group`
- `(access-list hardware ICMP filter)`
- `(access-list hardware IP protocol filter)`
- `(access-list hardware TCP UDP filter)`
- `(access-list standard named filter)`
- `show access-list (IPv4 Hardware ACLs)`
(access-list hardware ICMP filter)

**Overview**

Use this ACL filter to add a new ICMP filter entry to the current hardware access-list. The filter will match on any ICMP packet that has the specified source and destination IP addresses and ICMP type. The parameter *any* may be specified if an address does not matter and the ICMP type is an optional parameter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an ICMP filter entry from the current hardware access-list. You can specify the ICMP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its ICMP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the command, the *show access-list (IPv4 Hardware ACLs)* command.

**Syntax [icmp]**

```
[<sequence-number>] [deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror] icmp <source> <destination> [icmp <icmp-value>]
```

```
no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror} icmp <source> <destination> [icmp <icmp-value>]
```

```
no <sequence-number>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;sequence-number&gt;</code></td>
<td><code>&lt;1-65535&gt;</code></td>
</tr>
<tr>
<td>deny</td>
<td>Access-list rejects packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>Access-list permits packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>send-to-cpu</td>
<td>Specify packets to send to the CPU.</td>
</tr>
<tr>
<td>copy-to-cpu</td>
<td>Specify packets to copy to the CPU.</td>
</tr>
<tr>
<td>copy-to-mirror</td>
<td>Specify packets to copy to the mirror port.</td>
</tr>
<tr>
<td>icmp</td>
<td>ICMP packet type.</td>
</tr>
</tbody>
</table>
## IPV4 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS

### (access-list hardware ICMP filter)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;source&gt;</code></td>
<td>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:</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td>
</tr>
<tr>
<td><code>&lt;prefix&gt;</code></td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
<tr>
<td><code>host&lt;ip-addr&gt;</code></td>
<td>Matches a single source host with the IP address given by <code>&lt;ip-addr&gt;</code> in dotted decimal notation.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Matches any source IP address.</td>
</tr>
<tr>
<td><code>&lt;destination&gt;</code></td>
<td>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:</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.</td>
</tr>
<tr>
<td><code>&lt;prefix&gt;</code></td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
<tr>
<td><code>host&lt;ip-addr&gt;</code></td>
<td>Matches a single destination host with the IP address given by <code>&lt;ip-addr&gt;</code> in dotted decimal notation.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Matches any destination IP address.</td>
</tr>
<tr>
<td><code>icmp-type</code></td>
<td>The ICMP type.</td>
</tr>
<tr>
<td><code>&lt;icmp-value&gt;</code></td>
<td>The value of the ICMP type.</td>
</tr>
</tbody>
</table>

### Mode
IPv4 Hardware ACL Configuration

### Default
Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

### Usage
First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the `access-group` command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to incoming data packets.
An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** You must reach the prompt `awplus(config-ip-hw-acl)#` by running the `access-list hardware (named)` command, and entering an appropriate access-list name.

Hardware ACLs will *permit* access unless *explicitly denied* by an ACL action.

**Examples**

To add an access-list filter entry with a sequence number of 100 to the access-list named `my-list` that will permit ICMP packets with a source address of 192.168.1.0/24, any destination address and an icmp type of 5, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# 100 permit icmp 192.168.1.0/24 any icmp-type 5
```

To remove an access-list filter entry with a sequence number of 100 in the access-list named `my-list`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# no 100
```

**Related Commands**

- `access-list hardware (named)`
- `show running-config`
- `show access-list (IPv4 Hardware ACLs)`
(access-list hardware IP protocol filter)

**Overview**

Use this ACL filter to add an IP protocol type filter entry to the current hardware access-list. The filter will match on any IP packet that has the specified source and destination IP addresses and IP protocol type, or has the optionally specified source and destination MAC addresses. The parameter *any* may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The *no* variant of this command removes an IP protocol type filter entry from the current hardware access-list. You can specify the IP protocol type filter entry for removal by entering either its sequence number (e.g. *no 10*), or by entering its IP protocol type filter profile without specifying its sequence number.

Note that the sequence number can be found by running the `show access-list (IPv4 Hardware ACLs)` command.

**Syntax**

```
[any|ip|proto]
[<sequence-number>]
{deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror}
{any|ip|proto <ip-protocol>}
{<source>|dhcpsnooping|any}
{<destination>|any} [mac {
<mac-source-address>
<mac-source-mask>|any} {<mac-destination-address>
<mac-destination-mask>|any}]

no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror}
{any|ip|proto <ip-protocol>}
{<source>|dhcpsnooping}
{<destination>|any} [mac {
<mac-source-address>
<mac-source-mask>|any} {<mac-destination-address>
<mac-destination-mask>|any}]

no <sequence-number>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;sequence-number&gt;</code></td>
<td><code>&lt;1-65535&gt;</code> The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Access-list rejects packets of the type specified.</td>
</tr>
<tr>
<td>permit</td>
<td>Access-list allows packets of the type specified</td>
</tr>
<tr>
<td>send to cpu</td>
<td>Specify packets to send to the CPU.</td>
</tr>
<tr>
<td>copy to cpu</td>
<td>Specify packets to copy to the CPU.</td>
</tr>
<tr>
<td>copy to mirror</td>
<td>Specify packets to copy to the mirror port.</td>
</tr>
<tr>
<td>ip</td>
<td>IP packets.</td>
</tr>
<tr>
<td>any</td>
<td>Any packet.</td>
</tr>
<tr>
<td>proto <code>&lt;ip-protocol&gt;</code></td>
<td>The IP Protocol type specified by it protocol number <code>&lt;1-255&gt;</code>.</td>
</tr>
</tbody>
</table>
### IPV4 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS
(ACCESS-LIST HARDWARE IP PROTOCOL FILTER)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-protocol&gt;</code></td>
<td>The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority, <a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a>)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol Number</th>
<th>Protocol Description [RFC Reference]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet Control Message [RFC792]</td>
</tr>
<tr>
<td>2</td>
<td>Internet Group Management [RFC1112]</td>
</tr>
<tr>
<td>3</td>
<td>Gateway-to-Gateway [RFC823]</td>
</tr>
<tr>
<td>4</td>
<td>IP in IP [RFC2003]</td>
</tr>
<tr>
<td>5</td>
<td>Stream [RFC1190] [RFC1819]</td>
</tr>
<tr>
<td>6</td>
<td>TCP (Transmission Control Protocol) [RFC793]</td>
</tr>
<tr>
<td>8</td>
<td>EGP (Exterior Gateway Protocol) [RFC888]</td>
</tr>
<tr>
<td>9</td>
<td>IGP (Interior Gateway Protocol) [IANA]</td>
</tr>
<tr>
<td>11</td>
<td>Network Voice Protocol [RFC741]</td>
</tr>
<tr>
<td>17</td>
<td>UDP (User Datagram Protocol) [RFC768]</td>
</tr>
<tr>
<td>20</td>
<td>Host monitoring [RFC869]</td>
</tr>
<tr>
<td>27</td>
<td>RDP (Reliable Data Protocol) [RFC908]</td>
</tr>
<tr>
<td>28</td>
<td>IRTP (Internet Reliable Transaction Protocol) [RFC938]</td>
</tr>
<tr>
<td>29</td>
<td>ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]</td>
</tr>
<tr>
<td>30</td>
<td>Bulk Data Transfer Protocol [RFC969]</td>
</tr>
<tr>
<td>33</td>
<td>DCCP (Datagram Congestion Control Protocol) [RFC4340]</td>
</tr>
<tr>
<td>48</td>
<td>DSR (Dynamic Source Routing Protocol) [RFC4728]</td>
</tr>
<tr>
<td>50</td>
<td>ESP (Encap Security Payload) [RFC2406]</td>
</tr>
<tr>
<td>51</td>
<td>AH (Authentication Header) [RFC2402]</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><code>&lt;ip-protocol&gt;</code>(cont.)</td>
<td>54 NARP (NBMA Address Resolution Protocol) [RFC1735]</td>
</tr>
<tr>
<td></td>
<td>58 ICMP for IPv6 [RFC1883]</td>
</tr>
<tr>
<td></td>
<td>59 No Next Header for IPv6 [RFC1883]</td>
</tr>
<tr>
<td></td>
<td>60 Destination Options for IPv6 [RFC1883]</td>
</tr>
<tr>
<td></td>
<td>88 EIGRP (Enhanced Interior Gateway Routing Protocol)</td>
</tr>
<tr>
<td></td>
<td>89 OSPFv5 [RFC1583]</td>
</tr>
<tr>
<td></td>
<td>97 Ethernet-within-IP Encapsulation / RFC3378</td>
</tr>
<tr>
<td></td>
<td>98 Encapsulation Header / RFC1241</td>
</tr>
<tr>
<td></td>
<td>108 IP Payload Compression Protocol / RFC2393</td>
</tr>
<tr>
<td></td>
<td>112 Virtual Router Redundancy Protocol / RFC3768</td>
</tr>
<tr>
<td></td>
<td>134 RSVP-E2E-IGNORE / RFC3175</td>
</tr>
<tr>
<td></td>
<td>135 Mobility Header / RFC3775</td>
</tr>
<tr>
<td></td>
<td>136 UDPLite / RFC3828</td>
</tr>
<tr>
<td></td>
<td>137 MPLS-in-IP / RFC4023</td>
</tr>
<tr>
<td></td>
<td>138 MANET Protocols / RFC-ietf-manet-iana-07.txt</td>
</tr>
<tr>
<td></td>
<td>139-252 Unassigned / IANA</td>
</tr>
<tr>
<td></td>
<td>253 Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td></td>
<td>254 Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td></td>
<td>255 Reserved / IANA</td>
</tr>
<tr>
<td>dhcpsnooping</td>
<td>The source address learned from the DHCP Snooping binding database.</td>
</tr>
</tbody>
</table>
### IPV4 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS

#### ACCESS-LIST HARDWARE IP PROTOCOL FILTER

- **Parameter**: `<source>`
  - **Description**: 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`.

- **Parameter**: `<destination>`
  - **Description**: 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`.

- **Parameter**: `mac`
  - **Description**: Signifies a MAC and based hardware access-list.

- **Parameter**: `<mac-source-address>`
  - **Description**: The source host’s MAC address, entered in `HHHH.HHHH.HHHH` format.

- **Parameter**: `<mac-source-mask>`
  - **Description**: The source host’s MAC wildcard mask entered in `HHHH.HHHH.HHHH` format. where Hex FF = Ignore, and Hex 00 = Match.

- **Parameter**: `any`
  - **Description**: Matches any source MAC address.
**IPV4 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS**  
*(ACCESS-LIST HARDWARE IP PROTOCOL FILTER)*

### Mode
IPv4 Hardware ACL Configuration

### Default
Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

### Usage
First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the `access-group` command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to incoming data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** The access control list being configured is selected by running the `access-list hardware (named)` command, with the required access control list number, or name, but with no further parameters selected.

Hardware ACLs will permit access unless explicitly denied by an ACL action.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mac-destination-address&gt;</code></td>
<td>The destination host’s MAC address, entered in HHHH.HHHH.HHHH format.</td>
</tr>
<tr>
<td><code>&lt;mac-destination-mask&gt;</code></td>
<td>The destination host’s wildcard mask entered in HHHH.HHHH.HHHH format. where Hex FF = Ignore, and Hex 00 = Match.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Matches any destination MAC address.</td>
</tr>
</tbody>
</table>

### Examples
To add an access-list filter entry to the access-list named `my-list` that will permit any type of IP packet with a source address of 192.168.1.1 and any destination address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit ip 192.168.1.1/32 any
```

To add an access-list filter entry to the access-list named `my-list` that will permit any type of IP packet with a source address of 192.168.1.1 and a MAC source address of ffee.ddcc.bbaa with any IP and MAC destination address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit ip 192.168.1.1/32 any mac ffee.ddcc.bbaa any
```
To add an access-list filter entry to the access-list named `my-list` a filter that will deny all IGMP packets (protocol 2) from the 192.168.0.0 network with sequence number 50 in access-list, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# 50 deny proto 2 192.168.0.0/16 any
```

**Related Commands**
- `access-list hardware (named)`
- `show running-config`
- `show access-list (IPv4 Hardware ACLs)`
(access-list hardware MAC filter)

**Overview**
Use this ACL filter to add a MAC filter entry to the current hardware access-list. The filter will match on any IP packet that has the specified source and destination MAC addresses. The parameter *any* may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a MAC filter entry from the current hardware access-list. You can specify the MAC filter entry for removal by entering either its sequence number (e.g. **no 10**), or by entering its MAC filter profile without specifying its sequence number.

Note that the sequence number can be found by running the **show access-list (IPv4 Hardware ACLs)** command.

**Syntax**
```
[mac]
[<sequence-number>]
{deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror} mac
{<source-mac-address> <source-mac-mask>|any}
{<destination-mac-address> <destination-mac-mask>|any}
no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror} mac
{<source-mac-address> <source-mac-mask>|any}
{<destination-mac-address> <destination-mac-mask>|any}
no <sequence-number>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;sequence-number&gt;</code></td>
<td><code>&lt;1-65535&gt;</code> The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Specify packets to reject.</td>
</tr>
<tr>
<td>permit</td>
<td>Specify packets to accept.</td>
</tr>
<tr>
<td>send-to-cpu</td>
<td>Specify packets to send to the CPU.</td>
</tr>
<tr>
<td>copy-to-cpu</td>
<td>Specify packets to copy to the CPU.</td>
</tr>
<tr>
<td>copy-to-mirror</td>
<td>Specify packets to copy to the CPU.</td>
</tr>
<tr>
<td>mac</td>
<td>MAC address.</td>
</tr>
<tr>
<td><code>&lt;source-mac-address&gt;</code></td>
<td>The source MAC address of the packets. Enter this in the format <code>&lt;HHHH.HHHH.HHHH&gt;</code> where each H is a hexadecimal number that represents a 4 bit binary number.</td>
</tr>
<tr>
<td><code>&lt;source-mac-mask&gt;</code></td>
<td>The mask that will be applied to the source MAC addresses. Enter this in the format <code>&lt;HHHH.HHHH.HHHH&gt;</code> where each H is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either 0 or F. Where Hex FF = Ignore, and Hex 00 = Match.</td>
</tr>
</tbody>
</table>
IPV4 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS
(access-list hardware MAC filter)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>Any source MAC host.</td>
</tr>
<tr>
<td>&lt;destination-mac-address&gt;</td>
<td>The destination MAC address of the packets. Enter this in the format &lt;HHHH.HHHH.HHHH&gt; where each H is a hexadecimal number that represents a 4 bit binary number.</td>
</tr>
<tr>
<td>&lt;destination-mac-mask&gt;</td>
<td>The mask that will be applied to the destination MAC addresses. Enter this in the format &lt;HHHH.HHHH.HHHH&gt; where each H is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either 0 or F. Where Hex FF = Ignore, and Hex 00 = Match.</td>
</tr>
<tr>
<td>any</td>
<td>Any destination MAC host.</td>
</tr>
</tbody>
</table>

**Mode** IPv4 Hardware ACL Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage** First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the `access-group` command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to incoming data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** The access control list being configured is selected by running the `access-list hardware (named)` command with the required access control list number, or name, but with no further parameters selected.

Hardware ACLs will permit access unless explicitly denied by an ACL action.

**Examples** To add an access-list filter entry to the access-list named `my-list` that will permit packets with a source MAC address of 0000.00ab.1234 and any destination MAC address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit mac 0000.00ab.1234 0000.0000.0000 any
```

To remove an access-list filter entry that permit packets with a source MAC address of 0000.00ab.1234 and any destination MAC address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# no permit mac 0000.00ab.1234 0000.0000.0000 any
```
Related Commands

- access-group
- access-list hardware (named)
- show running-config
Overview

Use this ACL filter to add a TCP or UDP filter entry to the current hardware access-list. The filter will match on any TCP or UDP type packet that has the specified source and destination IP addresses. The parameter any may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The no variant of this command removes a TCP or UDP filter entry from the current hardware access-list. You can specify the TCP or UDP filter entry for removal by entering either its sequence number (e.g. no 10), or by entering its TCP or UDP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Hardware ACLs) command.

Syntax [tcp|udp]

```plaintext
[<sequence-number>]
{deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror} {tcp|udp}
[<source>|eq <sourceport>|gt <sourceport>|lt <sourceport>|ne <sourceport>|range <start-range> <end-range>]
[<destination>|eq <destport>|gt <destport>|lt <destport>|ne <destport>|range <start-range> <end-range>]
no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror} {tcp|udp} [<source>|eq <sourceport>|gt <sourceport>|lt <sourceport>|range <start-range> <end-range>]
[<destination>|eq <destport>|gt <destport>|lt <destport>|range <start-range> <end-range>]
no <sequence-number>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;sequence-number&gt;</code></td>
<td>The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Access-list rejects packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>Access-list permits packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>send-to-cpu</td>
<td>Specify packets to send to the CPU.</td>
</tr>
<tr>
<td>copy-to-cpu</td>
<td>Specify packets to copy to the CPU.</td>
</tr>
<tr>
<td>copy-to-mirror</td>
<td>Specify packets to copy to the mirror port.</td>
</tr>
<tr>
<td>tcp</td>
<td>TCP packets.</td>
</tr>
<tr>
<td>udp</td>
<td>UDP packets.</td>
</tr>
</tbody>
</table>
**IPV4 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS**

**ACCESS-LIST HARDWARE TCP UDP FILTER**

The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single source host with the IP address given by &lt;ip-addr&gt; in dotted decimal notation.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;/ &lt;prefix&gt;</td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt; &lt;reverse-mask&gt;</td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
</tbody>
</table>

The source TCP or UDP port number, specified as an integer between 0 and 65535.

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>Matches any destination IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single destination host with the IP address given by &lt;ip-addr&gt; in dotted decimal notation.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;/ &lt;prefix&gt;</td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt; &lt;reverse-mask&gt;</td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
</tbody>
</table>

eq               | Equal to.                                                                   |
lt                | Less than.                                                                  |
gt                | Greater than.                                                               |
ne                | Not equal to.                                                               |
IPV4 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS
(access-list hardware TCP UDP filter)

Mode
IPv4 Hardware ACL Configuration

Default
Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage
First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the access-group command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to incoming data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: The access control list being configured is selected by running the access-list hardware (named) command, with the required access control list number, or name, but with no further parameters selected.

Hardware ACLs will permit access unless explicitly denied by an ACL action.

Example
To add an access-list filter entry to access-list named my-hw-list that will permit TCP packets with a destination address of 192.168.1.1, a destination port of 80, and any source address, and source port, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-hw-list
awplus(config-ip-hw-acl)# permit tcp any 192.168.1.1/32 eq 80
```

Related
Commands
access-list hardware (named)
show running-config
show access-list (IPv4 Hardware ACLs)
commit (IPv4)

**Overview**  Use this command to commit the IPv4 ACL filter configuration entered at the console to the hardware immediately without exiting the IPv4 Hardware ACL Configuration mode.

This command forces the associated hardware and software IPv4 ACLs to synchronize.

**Syntax**  commit

**Mode**  IPv4 Hardware ACL Configuration

**Usage**  Normally, when an IPv4 hardware ACL is edited, the new configuration state of the IPv4 ACL is not written to hardware until you exit IPv4 Hardware ACL Configuration mode. By entering this command you can ensure that the current state of a hardware access-list that is being edited is written to hardware immediately.

Scripts typically do not include the exit command to exit configuration modes, potentially leading to IPv4 ACL filters in hardware not being correctly updated. Using this commit command in a configuration script after specifying an IPv4 hardware ACL filter ensures that it is updated in the hardware immediately.

**Example**  To update the hardware with the IPv4 ACL filter configuration, use the command:

```plaintext
awplus# configure terminal
awplus(config)# access-list hardware my-hw-list
awplus(config-ip-hw-acl)# commit
```

**Related Commands**  access-list hardware (named)
show access-list (IPv4 Hardware ACLs)

Overview
Use this command to display the specified access-list, or all access-lists if none have been specified. Note that only defined access-lists are displayed. An error message is displayed for an undefined access-list.

Syntax
show access-list
[<1-99>|<100-199>|<1300-1999>|<2000-2699>|<3000-3699>|<4000-4499>|<access-list-name>]

Parameter Description
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-99&gt;</td>
<td>IP standard access-list.</td>
</tr>
<tr>
<td>&lt;100-199&gt;</td>
<td>IP extended access-list.</td>
</tr>
<tr>
<td>&lt;1300-1999&gt;</td>
<td>IP standard access-list (standard - expanded range).</td>
</tr>
<tr>
<td>&lt;2000-2699&gt;</td>
<td>IP extended access-list (extended - expanded range).</td>
</tr>
<tr>
<td>&lt;3000-3699&gt;</td>
<td>Hardware IP access-list.</td>
</tr>
<tr>
<td>&lt;4000-4499&gt;</td>
<td>Hardware MAC access-list.</td>
</tr>
<tr>
<td>&lt;access-list-name&gt;</td>
<td>IP named access-list.</td>
</tr>
</tbody>
</table>

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
IPV4 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS
SHOW ACCESS-LIST (IPV4 HARDWARE ACLS)

Note the below error message if you attempt to show an undefined access-list:
```
awplus# show access-list 2
% Can't find access-list 2
```

**Related Commands**
- `access-list extended (named)`
- `access-list (hardware MAC numbered)`
- `access-list hardware (named)`
show interface access-group

Overview
Use this command to display the access groups attached to a port. If an access group is specified, then the output only includes the ports that the specified access group is attached to. If no access group is specified then this command displays all access groups that are attached to the ports that are specified with <port-list>.

Note that access group is the term given for an access-list when it is applied to an interface.

NOTE: This command will function on your switch in stand-alone mode. but is not supported when the device forms part of a VCStack.

Syntax
show interface <port-list> access-group
[<3000-3699>|<4000-4699>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>Specify the ports to display information. A port-list can be either:&lt;br&gt;- a switch port (e.g. port1.0.6) a static channel group (e.g. sa2) or a dynamic LACP channel group (e.g. po2)&lt;br&gt;- 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&lt;br&gt;- 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.</td>
</tr>
<tr>
<td>access group</td>
<td>Select the access group whose details you want to show.</td>
</tr>
<tr>
<td>&lt;3000-3699&gt;</td>
<td>Specifies the Hardware IP access-list.</td>
</tr>
<tr>
<td>&lt;4000-4699&gt;</td>
<td>Specifies the Hardware MAC access-list.</td>
</tr>
</tbody>
</table>

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 30-1: Example output from the show interface access-group command

<table>
<thead>
<tr>
<th>Interface port1.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-group 3000</td>
</tr>
<tr>
<td>access-group 3002</td>
</tr>
<tr>
<td>access-group 3001</td>
</tr>
</tbody>
</table>

Related Commands
access-group
Introduction

**Overview**
This chapter provides an alphabetical reference for the IPv4 Software Access Control List (ACL) commands, and contains detailed command information and command examples about IPv4 software ACLs as applied to Routing and Multicasting, which are not applied to interfaces.

For information about ACLs, see the **ACL Feature Overview** and **Configuration Guide**.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see the following references:

- the **Link Aggregation Feature Overview and Configuration Guide**.
- **Link Aggregation Commands**

**NOTE:** Text in parenthesis in command names indicates usage not keyword entry. For example, `access-list hardware (named)` indicates named IPv4 hardware ACLs entered as `access-list hardware <name>` where `<name>` is a placeholder not a keyword.

Parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as `(access-list standard numbered filter)` represents command entry in the format shown in the syntax: `{<sequence-number> | deny | permit} {<source> | host <host-address> | any}.

Software ACLs will **deny** access unless **explicitly permitted** by an **ACL action**.

**Sub-modes**
Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.
### Table 31-1: IPv4 Software Access List Commands and Prompts

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Command Mode</th>
<th>Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip prefix-list</td>
<td>Privileged Exec</td>
<td>awplus#</td>
</tr>
<tr>
<td>show ip access-list</td>
<td>Privileged Exec</td>
<td>awplus#</td>
</tr>
<tr>
<td>show ip prefix-list</td>
<td>Privileged Exec</td>
<td>awplus#</td>
</tr>
<tr>
<td>access-group</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>access-list (extended numbered)</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>access-list (standard named)</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>access-list (standard numbered)</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>maximum-access-list</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>dos</td>
<td>Interface Configuration</td>
<td>awplus(config-if)#</td>
</tr>
<tr>
<td>(access-list extended ICMP filter)</td>
<td>IPv4 Extended ACL Configuration</td>
<td>awplus(config-ip-ext-acl)#</td>
</tr>
<tr>
<td>(access-list extended IPfilter)</td>
<td>IPv4 Extended ACL Configuration</td>
<td>awplus(config-ip-ext-acl)#</td>
</tr>
<tr>
<td>(access-list extended IP protocol filter)</td>
<td>IPv4 Extended ACL Configuration</td>
<td>awplus(config-ip-ext-acl)#</td>
</tr>
<tr>
<td>(access-list extended TCP UDP filter)</td>
<td>IPv4 Extended ACL Configuration</td>
<td>awplus(config-ip-ext-acl)#</td>
</tr>
<tr>
<td>(access-list standard named filter)</td>
<td>IPv4 Standard ACL Configuration</td>
<td>awplus(config-ip-std-acl)#</td>
</tr>
<tr>
<td>(access-list standard numbered filter)</td>
<td>IPv4 Standard ACL Configuration</td>
<td>awplus(config-ip-std-acl)#</td>
</tr>
</tbody>
</table>
IPV4 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS

**Command List**

- “access-list extended (named)” on page 1336
- “access-list (extended numbered)” on page 1344
- “(access-list extended ICMP filter)” on page 1346
- “(access-list extended IP filter)” on page 1348
- “(access-list extended IP protocol filter)” on page 1351
- “(access-list extended TCP UDP filter)” on page 1356
- “access-list standard (named)” on page 1359
- “access-list (standard numbered)” on page 1361
- “(access-list standard named filter)” on page 1363
- “(access-list standard numbered filter)” on page 1365
- “clear ip prefix-list” on page 1367
- “dos” on page 1368
- “ip prefix-list” on page 1371
- “maximum-access-list” on page 1373
- “show access-list (IPv4 Software ACLs)” on page 1374
- “show dos interface” on page 1376
- “show ip access-list” on page 1379
- “show ip prefix-list” on page 1380
access-list extended (named)

**Overview**
This command configures an extended named access-list that permits or denies packets from specific source and destination IP addresses. You can either create an extended named ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Extended ACL Configuration mode for sequenced ACL filter entry after entering a list name.

The `no` variant of this command removes a specified extended named access-list.

**Syntax**

```
access-list extended <list-name>
no access-list extended <list-name>
```

**Table 31-2: Parameters in the access-list extended (named) command - icmp**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;list-name&gt;</code></td>
<td>A user-defined name for the access-list.</td>
</tr>
<tr>
<td>deny</td>
<td>The access-list rejects packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>The access-list permits packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td>icmp</td>
<td>The access-list matches only ICMP packets.</td>
</tr>
<tr>
<td>icmp-type</td>
<td>Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets.</td>
</tr>
</tbody>
</table>
Table 31-2: Parameters in the access-list extended (named) command - icmp

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;source&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single source host with the IP address given by &lt;ip-addr&gt; in dotted decimal notation.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;/&lt;prefix&gt;</td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
</tbody>
</table>

| <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>          | 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. |
**IPV4 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS**

**ACCESS-LIST EXTENDED (NAMED)**

---

**Table 31-2: Parameters in the access-list extended (named) command - icmp**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;type-number&gt;</td>
<td>The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type:</td>
</tr>
<tr>
<td>0</td>
<td>Echo replies.</td>
</tr>
<tr>
<td>3</td>
<td>Destination unreachable messages.</td>
</tr>
<tr>
<td>4</td>
<td>Source quench messages.</td>
</tr>
<tr>
<td>5</td>
<td>Redirect (change route) messages.</td>
</tr>
<tr>
<td>8</td>
<td>Echo requests.</td>
</tr>
<tr>
<td>11</td>
<td>Time exceeded messages.</td>
</tr>
<tr>
<td>12</td>
<td>Parameter problem messages.</td>
</tr>
<tr>
<td>13</td>
<td>Timestamp requests.</td>
</tr>
<tr>
<td>14</td>
<td>Timestamp replies.</td>
</tr>
<tr>
<td>15</td>
<td>Information requests.</td>
</tr>
<tr>
<td>16</td>
<td>Information replies.</td>
</tr>
<tr>
<td>17</td>
<td>Address mask requests.</td>
</tr>
<tr>
<td>18</td>
<td>Address mask replies.</td>
</tr>
<tr>
<td>log</td>
<td>Logs the results.</td>
</tr>
</tbody>
</table>

**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 31-3: Parameters in the access-list extended (named) command - tcp|udp**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;list-name&gt;</td>
<td>A user-defined name for the access-list.</td>
</tr>
<tr>
<td>deny</td>
<td>The access-list rejects packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>The access-list permits packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td>tcp</td>
<td>The access-list matches only TCP packets.</td>
</tr>
<tr>
<td>udp</td>
<td>The access-list matches only UDP packets.</td>
</tr>
</tbody>
</table>
### Table 31-3: Parameters in the access-list extended (named) command - tcp|udp

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;source&gt;</code></td>
<td>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:</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single source host with the IP address given by <code>&lt;ip-addr&gt;</code> in dotted decimal notation.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;/</code></td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td>
</tr>
<tr>
<td><code>&lt;prefix&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
<tr>
<td><code>&lt;reverse-mask&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;destination&gt;</code></td>
<td>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:</td>
</tr>
<tr>
<td>any</td>
<td>Matches any destination IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single destination host with the IP address given by <code>&lt;ip-addr&gt;</code> in dotted decimal notation.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;/</code></td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.</td>
</tr>
<tr>
<td><code>&lt;prefix&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
<tr>
<td><code>&lt;reverse-mask&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;sourceport&gt;</code></td>
<td>The source port number, specified as an integer between 0 and 65535.</td>
</tr>
<tr>
<td><code>&lt;destport&gt;</code></td>
<td>The destination port number, specified as an integer between 0 and 65535.</td>
</tr>
<tr>
<td>eq</td>
<td>Matches port numbers equal to the port number specified immediately after this parameter.</td>
</tr>
<tr>
<td>lt</td>
<td>Matches port numbers less than the port number specified immediately after this parameter.</td>
</tr>
<tr>
<td>gt</td>
<td>Matches port numbers greater than the port number specified immediately after this parameter.</td>
</tr>
</tbody>
</table>
**IPV4 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS**

**ACCESS-LIST EXTENDED (NAMED)**

**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 31-3: Parameters in the access-list extended (named) command - tcp|udp**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>list-name</code></td>
<td>A user-defined name for the access-list.</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>The access-list rejects packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>The access-list permits packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td><code>proto</code></td>
<td>Matches only a specified type of IP Protocol.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>The access-list matches any type of IP packet.</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>The access-list matches only IP packets.</td>
</tr>
<tr>
<td><code>source</code></td>
<td>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:</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Matches any source IP address.</td>
</tr>
<tr>
<td><code>host</code> <code>&lt;ip-addr&gt;</code></td>
<td>Matches a single source host with the IP address given by <code>&lt;ip-addr&gt;</code> in dotted decimal notation.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code> <code>/ </code>&lt;prefix&gt;`</td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code> <code>&lt;reverse-mask&gt;</code></td>
<td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
</tbody>
</table>

**Table 31-4: Parameters in the access-list extended (named) command - proto|ip|any**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;list-name&gt;</code></td>
<td>A user-defined name for the access-list.</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>The access-list rejects packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>The access-list permits packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td><code>proto</code></td>
<td>Matches only a specified type of IP Protocol.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>The access-list matches any type of IP packet.</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>The access-list matches only IP packets.</td>
</tr>
</tbody>
</table>
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.

The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority) [www.iana.org/assignments/protocol-numbers]

<table>
<thead>
<tr>
<th>Protocol Number</th>
<th>Protocol Description [RFC Reference]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet Control Message [RFC792]</td>
</tr>
<tr>
<td>2</td>
<td>Internet Group Management [RFC1112]</td>
</tr>
<tr>
<td>3</td>
<td>Gateway-to-Gateway [RFC823]</td>
</tr>
<tr>
<td>4</td>
<td>IP in IP [RFC2003]</td>
</tr>
<tr>
<td>5</td>
<td>Stream [RFC1190] [RFC1819]</td>
</tr>
<tr>
<td>6</td>
<td>TCP (Transmission Control Protocol) [RFC793]</td>
</tr>
<tr>
<td>8</td>
<td>EGP (Exterior Gateway Protocol) [RFC888]</td>
</tr>
<tr>
<td>9</td>
<td>IGP (Interior Gateway Protocol) [IANA]</td>
</tr>
<tr>
<td>11</td>
<td>Network Voice Protocol [RFC741]</td>
</tr>
<tr>
<td>17</td>
<td>UDP (User Datagram Protocol) [RFC768]</td>
</tr>
<tr>
<td>20</td>
<td>Host monitoring [RFC869]</td>
</tr>
<tr>
<td>27</td>
<td>RDP (Reliable Data Protocol) [RFC908]</td>
</tr>
<tr>
<td>28</td>
<td>IRTP (Internet Reliable Transaction Protocol) [RFC938]</td>
</tr>
<tr>
<td>29</td>
<td>ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]</td>
</tr>
<tr>
<td>30</td>
<td>Bulk Data Transfer Protocol [RFC969]</td>
</tr>
</tbody>
</table>

### Table 31-4: Parameters in the access-list extended (named) command - proto|ip|any (cont.)
**IPv4 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS**

**ACCESS-LIST EXTENDED (NAMED)**

---

**Mode** Global Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** Use this command when configuring access-list for filtering IP software packets. To enable backwards compatibility you can either create access-lists from within this command, or you can enter `access-list` followed by only the number. This latter

---

### Table 31-4: Parameters in the access-list extended (named) command - proto|ip|any (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-protocol&gt;</code></td>
<td>Protocol Number</td>
</tr>
<tr>
<td>(cont.)</td>
<td>Protocol Description [RFC Reference]</td>
</tr>
<tr>
<td>33</td>
<td>Datagram Congestion Control Protocol [RFC4340]</td>
</tr>
<tr>
<td>48</td>
<td>DSR (Dynamic Source Routing Protocol) [RFC4728]</td>
</tr>
<tr>
<td>50</td>
<td>ESP (Encap Security Payload) [RFC2406]</td>
</tr>
<tr>
<td>51</td>
<td>AH (Authentication Header) [RFC2402]</td>
</tr>
<tr>
<td>54</td>
<td>NARP (NBMA Address Resolution Protocol) [RFC1735]</td>
</tr>
<tr>
<td>88</td>
<td>EIGRP (Enhanced Interior Gateway Routing Protocol)</td>
</tr>
<tr>
<td>89</td>
<td>OSPFIGP [RFC1583]</td>
</tr>
<tr>
<td>97</td>
<td>Ethernet-within-IP Encapsulation / RFC3378</td>
</tr>
<tr>
<td>98</td>
<td>Encapsulation Header / RFC1241</td>
</tr>
<tr>
<td>108</td>
<td>IP Payload Compression Protocol / RFC2393</td>
</tr>
<tr>
<td>112</td>
<td>Virtual Router Redundancy Protocol / RFC3768</td>
</tr>
<tr>
<td>134</td>
<td>RSVP-E2E-IGNORE / RFC3175</td>
</tr>
<tr>
<td>135</td>
<td>Mobility Header / RFC3775</td>
</tr>
<tr>
<td>136</td>
<td>UDPLite / RFC3828</td>
</tr>
<tr>
<td>137</td>
<td>MPLS-in-IP / RFC4023</td>
</tr>
<tr>
<td>138</td>
<td>MANET Protocols / RFC-ietf-manet-iana-07.txt</td>
</tr>
<tr>
<td>139–252</td>
<td>Unassigned / IANA</td>
</tr>
<tr>
<td>253</td>
<td>Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td>254</td>
<td>Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td>255</td>
<td>Reserved / IANA</td>
</tr>
</tbody>
</table>

---

AlliedWare Plus™ Operating System - Version 5.4.5-0.x
method moves you to the IPv4 Extended ACL Configuration mode for the selected access-list number, and from here you can configure your access-lists by using the commands (access-list extended ICMP filter), (access-list extended IP filter), and (access-list extended IP protocol filter).

The table IPv4 Software Access List Commands and Prompts on page 1334 shows the prompts at which ACL commands are entered.

Note that packets must match both the source and the destination details.

**NOTE:** Software ACLs will *deny* access unless explicitly *permitted* by an ACL action.

### Examples

You can enter the extended named ACL in the Global Configuration mode together with the ACL filter entry on the same line, as shown below:

```bash
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:

```bash
awplus# configure terminal
awplus(config)# access-list extended TK
awplus(config-ip-ext-acl)# deny tcp 2.2.2.3/24 eq 14 3.3.3.4/24 eq 12 log
```
access-list (extended numbered)

**Overview**
This command configures an extended numbered access-list that permits or denies packets from specific source and destination IP addresses. You can either create an extended numbered ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Extended ACL Configuration mode for sequenced ACL filter entry after entering a list number.

The no variant of this command removes a specified extended named access-list.

**Syntax**

```
access-list {<100-199>|<2000-2699>}
no access-list {<100-199>|<2000-2699>}
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;100-199&gt;</td>
<td>IP extended access-list.</td>
</tr>
<tr>
<td>&lt;2000-2699&gt;</td>
<td>IP extended access-list (expanded range).</td>
</tr>
</tbody>
</table>

```
syntax [deny|permit] access-list {<100-199>|<2000-2699>} {deny|permit} ip <source> <destination>
no access-list {<100-199>|<2000-2699>} {deny|permit} ip <source> <destination>
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;100-199&gt;</td>
<td>IP extended access-list.</td>
</tr>
<tr>
<td>&lt;2000-2699&gt;</td>
<td>IP extended access-list (expanded range).</td>
</tr>
<tr>
<td>deny</td>
<td>Access-list rejects packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>Access-list permits packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>&lt;source&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single source host with the IP address given by &lt;ip-addr&gt; in dotted decimal notation.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt; &lt;reverse-mask&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Mode**  
Global Configuration

**Default**  
Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage**  
Use this command when configuring access-list for filtering IP software packets. To enable backwards compatibility you can either create access-lists from within this command, or you can enter `access-list` followed by only the number. This latter method moves you to the IPv4 Extended ACL Configuration mode for the selected access-list number, and from here you can configure your access-lists by using the commands `access-list extended ICMP filter`, `access-list extended IP filter`, and `access-list extended IP protocol filter`.

The table **IPv4 Software Access List Commands and Prompts** shows the prompts at which ACL commands are entered. See the relevant links shown for the **Related Commands**.

Note that packets must match both the source and the destination details.

**NOTE:** Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Examples**  
You can enter the extended named ACL in the Global Configuration mode together with the ACL filter entry on the same line, as in previous software releases as shown below:

```
awplus# configure terminal
awplus(config)# access-list 101 deny ip 172.16.10.0 0.0.0.255 any
```

Alternatively, you can enter the extended named ACL in Global Configuration mode before specifying the ACL filter entry in the IPv4 Extended ACL Configuration mode, as shown below:

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)# deny ip 172.16.10.0 0.0.0.255 any
```
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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;sequence-number&gt;</td>
<td>&lt;1-65535&gt; The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Access-list rejects packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>Access-list permits packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>icmp</td>
<td>ICMP packet type.</td>
</tr>
<tr>
<td>&lt;source&gt;</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>&lt;ip-addr&gt;/&lt;prefix&gt; An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td>
</tr>
<tr>
<td></td>
<td>any Matches any source IP address.</td>
</tr>
<tr>
<td>&lt;destination&gt;</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>&lt;ip-addr&gt;/&lt;prefix&gt; An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.</td>
</tr>
<tr>
<td></td>
<td>any Matches any destination IP address.</td>
</tr>
<tr>
<td>icmp-type</td>
<td>The ICMP type.</td>
</tr>
</tbody>
</table>
### Mode
IPv4 Extended ACL Configuration

### Default
Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

### Usage
An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** The access control list being configured is selected by running the `access-list (extended numbered)` command or the `access-list extended (named)` command, with the required access control list number, or name - but with no further parameters selected.

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

### Examples
To add a new entry in access-list called `my-list` that will reject ICMP packets from 10.0.0.1 to 192.168.1.1, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny icmp 10.0.0.1/32 192.168.1.1/32
```

Use the following commands to add a new filter at sequence number 5 position of the access-list called `my-list`. The filter will accept the ICMP type 8 packets from 10.1.1.0/24 network, to 192.168.1.0 network:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit icmp 10.1.1.0/24 192.168.1.0/24 icmp-type 8
```
(access-list extended IP filter)

**Overview**

Use this ACL filter to add a new IP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP filter entry from the current extended access-list. You can specify the IP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the `show access-list (IPv4 Software ACLs)` command.

**Syntax [ip]**

```
[<sequence-number>]  {deny|permit} ip <source> <destination>
no {deny|permit} ip <source> <destination>
no <sequence-number>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;sequence-number&gt;</code></td>
<td><code>&lt;1-65535&gt;</code> The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Access-list rejects packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>Access-list permits packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td><code>&lt;source&gt;</code></td>
<td>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:</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
<tr>
<td>host&lt;ip-addr&gt;</td>
<td>Matches a single source host with the IP address given by <code>&lt;ip-addr&gt;</code> in dotted decimal notation.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>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.</td>
</tr>
</tbody>
</table>
**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**  
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**  
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**  
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
```
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]

\[
\text{[\text{<sequence-number>}] \{deny|permit\} proto \text{<ip-protocol>} \text{<source>} \text{<destination>} \{log\}}
\]

\[
\text{no \{deny|permit\} proto \text{<ip-protocol>} \text{<source>} \text{<destination>} \{log\}}
\]

\[
\text{no \text{<sequence-number>}}
\]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;sequence-number&gt;</td>
<td>1-65535&lt;br&gt; The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Access-list rejects packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>Access-list permits packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>proto</td>
<td>The IP Protocol type specified by its protocol number 1-255.</td>
</tr>
<tr>
<td>&lt;ip-protocol&gt;</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&lt;ip-protocol&gt;</td>
<td>The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority [<a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a>]).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol Number</th>
<th>Protocol Description [RFC Reference]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet Control Message [RFC792]</td>
</tr>
<tr>
<td>2</td>
<td>Internet Group Management [RFC1112]</td>
</tr>
<tr>
<td>3</td>
<td>Gateway-to-Gateway [RFC823]</td>
</tr>
<tr>
<td>4</td>
<td>IP in IP [RFC2003]</td>
</tr>
<tr>
<td>5</td>
<td>Stream [RFC1190] [RFC1819]</td>
</tr>
<tr>
<td>6</td>
<td>TCP (Transmission Control Protocol) [RFC793]</td>
</tr>
<tr>
<td>8</td>
<td>EGP (Exterior Gateway Protocol) [RFC888]</td>
</tr>
<tr>
<td>9</td>
<td>IGP (Interior Gateway Protocol) [IANA]</td>
</tr>
<tr>
<td>11</td>
<td>Network Voice Protocol [RFC741]</td>
</tr>
</tbody>
</table>
### Parameter List (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>UDP (User Datagram Protocol) [RFC768]</td>
</tr>
<tr>
<td>20</td>
<td>Host monitoring [RFC869]</td>
</tr>
<tr>
<td>27</td>
<td>RDP (Reliable Data Protocol) [RFC908]</td>
</tr>
<tr>
<td>28</td>
<td>IRTP (Internet Reliable Transaction Protocol) [RFC938]</td>
</tr>
<tr>
<td>29</td>
<td>ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]</td>
</tr>
<tr>
<td>30</td>
<td>Bulk Data Transfer Protocol [RFC969]</td>
</tr>
<tr>
<td>33</td>
<td>DCCP (Datagram Congestion Control Protocol) [RFC4340]</td>
</tr>
<tr>
<td>48</td>
<td>DSR (Dynamic Source Routing Protocol) [RFC4728]</td>
</tr>
<tr>
<td>50</td>
<td>ESP (Encap Security Payload) [RFC2406]</td>
</tr>
<tr>
<td>51</td>
<td>AH (Authentication Header) [RFC2402]</td>
</tr>
<tr>
<td>54</td>
<td>NARP (NBMA Address Resolution Protocol) [RFC1735]</td>
</tr>
<tr>
<td>88</td>
<td>EIGRP (Enhanced Interior Gateway Routing Protocol)</td>
</tr>
<tr>
<td>89</td>
<td>OSPFIGP [RFC1583]</td>
</tr>
<tr>
<td>97</td>
<td>Ethernet-within-IP Encapsulation / RFC3378</td>
</tr>
<tr>
<td>98</td>
<td>Encapsulation Header / RFC1241</td>
</tr>
<tr>
<td>108</td>
<td>IP Payload Compression Protocol / RFC2393</td>
</tr>
<tr>
<td>112</td>
<td>Virtual Router Redundancy Protocol / RFC3768</td>
</tr>
<tr>
<td>134</td>
<td>RSVP-E2E-IGNORE / RFC3175</td>
</tr>
<tr>
<td>135</td>
<td>Mobility Header / RFC3775</td>
</tr>
<tr>
<td>136</td>
<td>UDPLite / RFC3828</td>
</tr>
<tr>
<td>137</td>
<td>MPLS-in-IP / RFC4023</td>
</tr>
<tr>
<td>138</td>
<td>MANET Protocols / RFC-ietf-manet-iana-07.txt</td>
</tr>
<tr>
<td>139-252</td>
<td>Unassigned / IANA</td>
</tr>
<tr>
<td>253</td>
<td>Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td>254</td>
<td>Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td>255</td>
<td>Reserved / IANA</td>
</tr>
</tbody>
</table>
IPV4 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS
(ACCESS-LIST EXTENDED IP PROTOCOL FILTER)

Mode
IPv4 Extended ACL Configuration

Default
Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage
An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** The access control list being configured is selected by running the `access-list (extended numbered)` command or the `access-list extended (named)` command, with the required access control list number, or name - but with no further parameters selected.

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Example 1 [creating a list]
Use the following commands to add a new access-list filter entry to the access-list named `my-list` that will reject IP packets from source address 10.1.1.1/32 to destination address 192.168.1.1/32:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny ip 10.1.1.1/32 192.168.1.1/32
```
**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 192.168.1.1/24:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit ip 10.10.1.1/24 192.168.1.1/24
```
(access-list extended TCP UDP filter)

**Overview**

Use this ACL filter to add a new TCP or UDP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a TCP or UDP filter entry from the current extended access-list. You can specify the TCP or UDP filter entry for removal by entering either its sequence number (e.g. **no 10**), or by entering its TCP or UDP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the **show access-list (IPv4 Software ACLs)** command.

**Syntax [tcp|udp]**

```
[<sequence-number>] {deny|permit} {tcp|udp} <source> {eq <sourceport> | 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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;sequence-number&gt;</code></td>
<td><code>&lt;1-65535&gt;</code> The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Access-list rejects packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>Access-list permits packets that match the source and destination filtering specified with this command.</td>
</tr>
<tr>
<td>tcp</td>
<td>The access-list matches only TCP packets.</td>
</tr>
<tr>
<td>udp</td>
<td>The access-list matches only UDP packets.</td>
</tr>
<tr>
<td><code>&lt;source&gt;</code></td>
<td>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:</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;/prefix</code></td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
<tr>
<td><code>&lt;sourceport&gt;</code></td>
<td>The source port number, specified as an integer between 0 and 65535.</td>
</tr>
</tbody>
</table>
IPV4 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS
(access-list extended TCP UDP FILTER)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;destination&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;/</td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.</td>
</tr>
<tr>
<td>&lt;prefix&gt;</td>
<td></td>
</tr>
<tr>
<td>any</td>
<td>Matches any destination IP address.</td>
</tr>
<tr>
<td>&lt;destport&gt;</td>
<td>The destination port number, specified as an integer between 0 and 65535.</td>
</tr>
<tr>
<td>eq</td>
<td>Matches port numbers equal to the port number specified immediately after this parameter.</td>
</tr>
<tr>
<td>lt</td>
<td>Matches port numbers less than the port number specified immediately after this parameter.</td>
</tr>
<tr>
<td>gt</td>
<td>Matches port numbers greater than the port number specified immediately after this parameter.</td>
</tr>
<tr>
<td>ne</td>
<td>Matches port numbers not equal to the port number specified immediately after this parameter.</td>
</tr>
<tr>
<td>log</td>
<td>Log the results.</td>
</tr>
</tbody>
</table>

**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
```
Overview
This command configures a standard named access-list that permits or denies packets from a specific source IP address. You can either create a standard named ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Standard ACL Configuration mode for sequenced ACL filter entry after first entering an access-list name.

The no variant of this command removes a specified standard named access-list.

Syntax
access-list standard <standard-access-list-name>
no access-list standard <standard-access-list-name>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;standard-access-list-name&gt;</td>
<td>Specify a name for the standard access-list.</td>
</tr>
</tbody>
</table>

Syntax
access-list standard <standard-access-list-name> {deny|permit} <source>
no access-list standard <standard-access-list-name> {deny|permit} <source>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;standard-access-list-name&gt;</td>
<td>Specify a name for the standard access-list.</td>
</tr>
<tr>
<td>deny</td>
<td>The access-list rejects packets that match the source filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>The access-list permits packets that match the source filtering specified with this command.</td>
</tr>
<tr>
<td>&lt;source&gt;</td>
<td>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:</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;/prefix</td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
</tbody>
</table>

Mode
Global Configuration

Default
Any traffic controlled by a software ACL that does not explicitly match a filter is denied.
**Usage**

Use this command when configuring a standard named access-list for filtering IP software packets. For backwards compatibility you can either create the access-list from within this command, or you can enter this command followed by only the standard access-list name then enter. This latter method moves you to the IPv4 Standard ACL Configuration mode for the selected standard named access-list, and from here you can configure the deny or permit filters for this selected standard named access-list.

See the table [IPv4 Software Access List Commands and Prompts](#) which shows the prompts at which ACL commands are entered. See the relevant links shown for the Related Commands.

**NOTE:** Software ACLs will **deny access unless explicitly permitted** by an ACL action.

**Examples**

To define a standard access-list named `my-list` and deny any packets from any source, use the commands:

```
awplus# configure terminal
awplus(config)# access-list standard my-list deny any
```

Alternatively, to define a standard access-list named `my-list` and enter the IPv4 Standard ACL Configuration mode to deny any packets from any source, use the commands:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# 5 deny any
```
access-list (standard numbered)

**Overview**
This command configures a standard numbered access-list that permits or denies packets from a specific source IP address. You can either create a standard numbered ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Standard ACL Configuration mode for sequenced ACL filter entry after first entering an access-list number.

The **no** variant of this command removes a specified standard numbered access-list.

**Syntax**
```plaintext
[<list-number>]
access-list {<1-99>|<1300-1999>}
no access-list {<1-99>|<1300-1999>}
```

**Parameter**
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-99&gt;</td>
</tr>
<tr>
<td>&lt;1300-1999&gt;</td>
</tr>
</tbody>
</table>

**Syntax [deny|permit]**
```plaintext
access-list {<1-99>|<1300-1999>} {deny|permit} <source>
no access-list {<1-99>|<1300-1999>} {deny|permit} <source>
```

**Parameter**
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-99&gt;</td>
</tr>
<tr>
<td>&lt;1300-1999&gt;</td>
</tr>
<tr>
<td>deny</td>
</tr>
<tr>
<td>permit</td>
</tr>
<tr>
<td>&lt;source&gt;</td>
</tr>
<tr>
<td>ip-addr</td>
</tr>
<tr>
<td>reverse-mask</td>
</tr>
<tr>
<td>any</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Default**
Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage**
Use this command when configuring a standard numbered access-list for filtering IP software packets. For backwards compatibility you can either create the access-list from within this command, or you can enter this command followed by
only the standard access-list name. This moves you to the IPv4 Standard ACL Configuration mode for the selected standard numbered access-list, and from here you can configure the deny or permit filters for this selected standard numbered access-list.

The table **IPv4 Software Access List Commands and Prompts** shows the prompts at which ACL commands are entered.

**NOTE:** Software ACLs will **deny** access unless explicitly permitted by an ACL action.

**Examples**

To create ACL number 67 that will deny packets from subnet 172.16.10.0, use the commands:

awplus# configure terminal
awplus(config)# access-list 67 deny 172.16.10.0 0.0.0.255

Alternatively, to enter the IPv4 Standard ACL Configuration mode to create the ACL filter and deny packets from subnet 172.16.10.0 for the standard numbered access-list 67, use the commands:

awplus# configure terminal
awplus(config)# access-list 67
awplus(config-ip-std-acl)# deny 172.16.10.0 0.0.0.255

**Related Commands**

(assess-list standard named filter)

- show running-config
- show ip access-list
(access-list standard named filter)

Overview  This ACL filter adds a source IP address filter entry to a current named standard access-list. If the sequence number is specified, the new filter entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The no variant of this command removes a source IP address filter entry from the current named standard access-list. You can specify the source IP address filter entry for removal by entering either its sequence number (e.g. no 10), or by entering its source IP address filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax  

```
[<sequence-number>] {deny|permit} {<source> [exact-match]|any}
no {deny|permit} {<source> [exact-match]|any}
no <sequence-number>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;sequence-number&gt;</td>
<td>&lt;1-65535&gt;</td>
</tr>
<tr>
<td></td>
<td>The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Access-list rejects packets of the source filtering specified.</td>
</tr>
<tr>
<td>permit</td>
<td>Access-list allows packets of the source filtering specified.</td>
</tr>
<tr>
<td>&lt;source&gt;</td>
<td>The source address of the packets. You can specify either a subnet or all sources. The following are the valid formats for specifying the source:</td>
</tr>
<tr>
<td></td>
<td>&lt;ip-addr&gt;/</td>
</tr>
<tr>
<td></td>
<td>&lt;prefix&gt;</td>
</tr>
<tr>
<td></td>
<td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.</td>
</tr>
<tr>
<td></td>
<td>&lt;ip-addr&gt;</td>
</tr>
<tr>
<td></td>
<td>An IPv4 address in a.b.c.d format.</td>
</tr>
<tr>
<td>exact-match</td>
<td>Specify an exact IP prefix to match on.</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
</tbody>
</table>

Mode  IPv4 Standard ACL Configuration

Default  Any traffic controlled by a software ACL that does not explicitly match a filter is denied.
**Usage**

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

*NOTE:* The access control list being configured is selected by running the `access-list standard (named)` command with the required access control list number, or name, but with no further parameters selected.

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Examples**

Use the following commands to add a new filter entry to `access-list my-list` that will reject IP address 10.1.1.1:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# deny 10.1.1.1/32
```

Use the following commands to insert a new filter entry into `access-list my-list` at sequence position number 15 that will accept IP network 10.1.2.0:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# 15 permit 10.1.2.0/24
```

**Related Commands**

- `access-list standard (named)`
- `show running-config`
- `show ip access-list`
Overview

This ACL filter adds a source IP address filter entry to a current standard numbered access-list. If a sequence number is specified, the new filter entry is inserted at the specified location. Otherwise, the new filter entry is added at the end of the access-list.

The no variant of this command removes a source IP address filter entry from the current standard numbered access-list. You can specify the source IP address filter entry for removal by entering either its sequence number (e.g. no 10), or by entering its source IP address filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax

```
[<sequence-number>] {deny|permit} [<source>|host <host-address>|any]
no {deny|permit} [<source>|host <host-address>|any]
no <sequence-number>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;sequence-number&gt;</td>
<td>&lt;1-65535&gt; The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Access-list rejects packets of the type specified.</td>
</tr>
<tr>
<td>permit</td>
<td>Access-list allows packets of the type specified.</td>
</tr>
<tr>
<td>&lt;source&gt;</td>
<td>The source address of the packets. You can specify either a subnet or all sources. The following are the valid formats for specifying the source:</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>Enter a reverse mask for the source address in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td>
</tr>
<tr>
<td>&lt;reverse-mask&gt;</td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>A single source host.</td>
</tr>
<tr>
<td>&lt;host-address&gt;</td>
<td>Single source host address.</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IP address.</td>
</tr>
</tbody>
</table>

Mode

IPv4 Standard ACL Configuration

Default

Any traffic controlled by a software ACL that does not explicitly match a filter is denied.
**Usage**  
An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** The access control list being configured is selected by running the `access-list standard (named)` command with the required access control list number, or name, but with no further parameters selected.

*Software ACLs will deny access unless explicitly permitted by an ACL action.*

**Example**  
To add a new entry accepting the IP network 10.1.1.0/24 at the sequence number 15 position, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 99
awplus(config-ip-std-acl)# 15 permit 10.1.2.0 0.0.0.255
```

**Related Commands**
- `access-list (standard numbered)`
- `show running-config`
- `show ip access-list`
**clear ip prefix-list**

**Overview**  
Use this command to reset the hit count to zero in the prefix-list entries.

**Syntax**  
clear ip prefix-list [<list-name>] [<ip-address>/<mask>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;list-name&gt;</td>
<td>The name of the prefix-list.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;/&lt;mask&gt;</td>
<td>The IP prefix and length.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec

**Example**  
To clear a prefix-list named List1:

```
awplus# clear ip prefix-list List1
```
**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}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dos</td>
<td>Denial-Of-Service.</td>
</tr>
<tr>
<td>ipoptions</td>
<td>IP Options attack.</td>
</tr>
<tr>
<td>land</td>
<td>Land attack.</td>
</tr>
<tr>
<td>ping-of-death</td>
<td>Large ping attack.</td>
</tr>
<tr>
<td>smurf</td>
<td>Ping to broadcast address.</td>
</tr>
<tr>
<td>broadcast</td>
<td>Broadcast.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>Local IP Broadcast Address.</td>
</tr>
<tr>
<td>synflood</td>
<td>SYN flood attack.</td>
</tr>
<tr>
<td>teardrop</td>
<td>IP fragmentation attack.</td>
</tr>
<tr>
<td>action</td>
<td>Action.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shutdown port.</td>
</tr>
<tr>
<td>trap</td>
<td>Trap to SNMP.</td>
</tr>
<tr>
<td>mirror</td>
<td>Send packets to mirror port.</td>
</tr>
</tbody>
</table>

**Mode**

Interface Configuration for a switch port interface.

**Default**

DoS attack detection is not configured by default on any switch port interface.

**Usage**

See the below table for more information about the DoS attacks recognized by this command:
### IPV4 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS

#### DOS

<table>
<thead>
<tr>
<th>Type of DoS attack</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipoptions</td>
<td>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.</td>
</tr>
<tr>
<td>land</td>
<td>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.</td>
</tr>
<tr>
<td>ping-of-death</td>
<td>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.</td>
</tr>
<tr>
<td>smurf</td>
<td>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.</td>
</tr>
<tr>
<td>synflood</td>
<td>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.</td>
</tr>
<tr>
<td>teardrop</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Examples**

To configure **smurf** DoS detection on port1.0.1, and shutdown the interface if an attack is detected, use the commands:

```bash
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:

```bash
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:

```bash
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:

```bash
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:

```bash
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:

```bash
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos teardrop action shutdown
```

**Related Commands**

```
show dos interface
```
IPV4 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS
IP PREFIX-LIST

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
```

**Mode**

Global Configuration

**Usage**

When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the `seq` parameter and place common permits or denials towards the top of the list. If you do not use the `seq` parameter, the sequence values are generated in a sequence of 5.

The parameters `ge` and `le` specify the range of the prefix lengths to be matched. When setting these parameters, set the `le` value to be less than 32, and the `ge` value to be less than or equal to the `le` value and greater than the ip-prefix mask length.

Prefix lists implicitly exclude prefixes that are not explicitly permitted in the prefix list. This means if a prefix that is being checked against the prefix list reaches the end of the prefix list without matching a permit or deny, this prefix will be denied.
Example  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
**maximal-access-list**

**Overview**
Sets the maximum number of filters that can be added to any access-list. These are access-lists within the ranges <1-199>, <1300-1999> and <2000-2699> and named standard and extended access-lists.

The **no** variant of this command removes the limit on the number of filters that can be added to a software access-list.

**Syntax**
```
maximum-access-list <1-4294967294>
no maximum-access-list
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4294967294&gt;</td>
<td>Filter range.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Example**
To set the maximum number of software filters to 200:
```
awplus# configure terminal
awplus(config)# maximum-access-list 200
```
show access-list (IPv4 Software ACLs)

Overview
Use this command to display the specified access-list, or all access-lists if none have been specified. Note that only defined access-lists are displayed. An error message is displayed for an undefined access-list.

Syntax
show access-list
[<1-99>|<100-199>|<1300-1999>|<2000-2699>|<3000-3699>|<4000-4499>|<access-list-name>]

Mode
User Exec and Privileged Exec

Examples
To show all access-lists configured on the switch:

awplus# show access-list

Standard IP access-list 1
  deny 172.16.2.0, wildcard bits 0.0.0.255
Standard IP access-list 20
  deny 192.168.10.0, wildcard bits 0.0.0.255
  deny 192.168.12.0, wildcard bits 0.0.0.255
Hardware IP access-list 3001
  permit ip 192.168.20.0 255.255.255.0 any
Hardware IP access-list 3020
  permit tcp any 192.0.2.0/24
awplus# show access-list 20

To show the access-list with an ID of 20:

awplus# show access-list 20

Standard IP access-list 20
  deny 192.168.10.0, wildcard bits 0.0.0.255
  deny 192.168.12.0, wildcard bits 0.0.0.255
Note the below error message if you attempt to show an undefined access-list:

```
awplus# show access-list 2
% Can't find access-list 2
```

**Related Commands**
- `access-list standard (named)`
- `access-list (standard numbered)`
- `access-list (extended numbered)`
show 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>}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>Specify the switch port or port list to display DoS configuration options set with the dos command.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Output**  Figure 31-1: Example output from the show dos interface command prior to a DoS attack

```
awplus#configure terminal
Enter configuration commands, one per line. End with CTNL/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 31-2: 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
neardrop            : Disabled
awplus#
```

Table 31-5: Parameters in the **show dos interface** command output:

<table>
<thead>
<tr>
<th>Type of DoS attack</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port status</td>
<td>Displays <strong>Enabled</strong> when the port is configured as being administratively up after issuing the <strong>no shutdown</strong> command. Displays <strong>Disabled</strong> when the port is configured as being administratively down with the <strong>shutdown</strong> command.</td>
</tr>
<tr>
<td>ipoptions</td>
<td>Displays <strong>Enabled</strong> when the <strong>ipoptions</strong> parameter is configured with the <strong>dos</strong> command, plus the action (<strong>Shutdown port</strong>, <strong>Mirror port</strong>, or <strong>Trap port</strong>) and the number of instances of any <strong>ipoptions</strong> DoS attacks that have occurred on the interface. Displays <strong>Disabled</strong> when the <strong>ipoptions</strong> parameter is not configured with the <strong>dos</strong> command.</td>
</tr>
<tr>
<td>land</td>
<td>Displays <strong>Enabled</strong> when the <strong>land</strong> parameter is configured with the <strong>dos</strong> command, plus the action (<strong>Shutdown port</strong>, <strong>Mirror port</strong>, or <strong>Trap port</strong>) and the number of instances of any <strong>land</strong> DoS attacks that have occurred on the interface. Displays <strong>Disabled</strong> when the <strong>land</strong> parameter is not configured with the <strong>dos</strong> command.</td>
</tr>
<tr>
<td>ping-of-death</td>
<td>Displays <strong>Enabled</strong> when the <strong>ping-of-death</strong> parameter is configured with the <strong>dos</strong> command, plus the action (<strong>Shutdown port</strong>, <strong>Mirror port</strong>, or <strong>Trap port</strong>) and the number of instances of any <strong>ping-of-death</strong> DoS attacks that have occurred on the interface. Displays <strong>Disabled</strong> when the <strong>ping-of-death</strong> parameter is not configured with the <strong>dos</strong> command.</td>
</tr>
</tbody>
</table>
Table 31-5: Parameters in the `show dos interface` command output: (cont.)

<table>
<thead>
<tr>
<th>Type of DoS attack</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>smurf</td>
<td>Displays Enabled when the <code>smurf</code> parameter is configured with the <code>dos</code> command, plus the action (Shutdown port, Mirror port, or Trap port) and the number of instances of any <code>smurf</code> DoS attacks that have occurred on the interface. Displays Disabled when the <code>smurf</code> parameter is not configured with the <code>dos</code> command.</td>
</tr>
<tr>
<td>synflood</td>
<td>Displays Enabled when the <code>synflood</code> parameter is configured with the <code>dos</code> command, plus the action (Shutdown port, Mirror port, or Trap port) and the number of instances of any <code>synflood</code> DoS attacks that have occurred on the interface. Displays Disabled when the <code>synflood</code> parameter is not configured with the <code>dos</code> command.</td>
</tr>
<tr>
<td>teardrop</td>
<td>Displays Enabled when the <code>teardrop</code> parameter is configured with the <code>dos</code> command, plus the action (Shutdown port, Mirror port, or Trap port) and the number of instances of any <code>teardrop</code> DoS attacks that have occurred on the interface. Displays Disabled when the <code>teardrop</code> parameter is not configured with the <code>dos</code> command.</td>
</tr>
</tbody>
</table>
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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-99&gt;</td>
<td>IP standard access-list.</td>
</tr>
<tr>
<td>&lt;100-199&gt;</td>
<td>IP extended access-list.</td>
</tr>
<tr>
<td>&lt;1300-1999&gt;</td>
<td>IP standard access-list (expanded range).</td>
</tr>
<tr>
<td>&lt;2000-2699&gt;</td>
<td>IP extended access-list (expanded range).</td>
</tr>
<tr>
<td>&lt;access-list-name&gt;</td>
<td>IP named access-list.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**

```
awplus# show ip access-list
```

**Output**  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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>Specify the name of a prefix list in this placeholder.</td>
</tr>
<tr>
<td>detail</td>
<td>Specify this parameter to show detailed output for all IPv4 prefix lists.</td>
</tr>
<tr>
<td>summary</td>
<td>Specify this parameter to show summary output for all IPv4 prefix lists.</td>
</tr>
</tbody>
</table>

**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
 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:

- the Link Aggregation Feature Overview and Configuration Guide.
- Link Aggregation Commands

Note that text in parenthesis in command names indicates usage not keyword entry. For example, `ipv6-access-list (named)` indicates named IPv6 ACLs entered as `ipv6-access-list <name>` where `<name>` is a placeholder not a keyword.

Note also that parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as `(ipv6 access-list standard IPv6 filter)` represents command entry in the format shown in the syntax `[:<sequence-number>] [deny|permit] <IPv6-source-address/prefix-length>|any`.

**NOTE:** Hardware ACLs will permit access unless explicitly denied by an ACL action.

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 32-1: IPv6 Hardware Access List Commands and Prompts

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Command Mode</th>
<th>Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 access-list (IPv6 Hardware ACLs)</code></td>
<td>Privileged Exec</td>
<td><code>awplus#</code></td>
</tr>
<tr>
<td><code>ipv6 access-list (named)</code></td>
<td>Global Configuration</td>
<td><code>awplus(config)#</code></td>
</tr>
<tr>
<td><code>(ipv6 access-list named ICMP filter)</code></td>
<td>Global Configuration</td>
<td><code>awplus(config)#</code></td>
</tr>
<tr>
<td><code>ipv6 traffic-filter</code></td>
<td>Interface Configuration</td>
<td><code>awplus(config-if)#</code></td>
</tr>
<tr>
<td><code>commit (IPv6)</code></td>
<td>IPv6 Hardware ACL</td>
<td><code>awplus(config-ipv6-hw-acl)#</code></td>
</tr>
<tr>
<td><code>(ipv6 access-list named ICMP filter)</code></td>
<td>IPv6 Hardware ACL</td>
<td><code>awplus(config-ipv6-hw-acl)#</code></td>
</tr>
<tr>
<td><code>(ipv6 access-list named protocol filter)</code></td>
<td>IPv6 Hardware ACL</td>
<td><code>awplus(config-ipv6-hw-acl)#</code></td>
</tr>
<tr>
<td><code>(ipv6 access-list named TCP UDP filter)</code></td>
<td>IPv6 Hardware ACL</td>
<td><code>awplus(config-ipv6-hw-acl)#</code></td>
</tr>
</tbody>
</table>

### Command List

- “commit (IPv6)” on page 1382
- “ipv6 access-list (named)” on page 1383
- “(ipv6 access-list named ICMP filter)” on page 1385
- “(ipv6 access-list named protocol filter)” on page 1388
- “(ipv6 access-list named TCP UDP filter)” on page 1392
- “ipv6 traffic-filter” on page 1397
- “show ipv6 access-list (IPv6 Hardware ACLs)” on page 1399
commit (IPv6)

**Overview**  Use this command to commit the IPv6 ACL filter configuration entered at the console to the hardware immediately without exiting the IPv6 Hardware ACL Configuration mode.

This command forces the associated hardware and software IPv6 ACLs to synchronize.

**Syntax**  commit

**Mode**  IPv6 Hardware ACL Configuration

**Usage**  Normally, when an IPv6 hardware ACL is edited, the new configuration state of the IPv6 ACL is not written to hardware until you exit IPv6 Hardware ACL Configuration mode. By entering this command you can ensure that the current state of a hardware access-list that is being edited is written to hardware immediately.

Scripts typically do not include the `exit` command to exit configuration modes, potentially leading to IPv6 ACL filters in hardware not being correctly updated. Using this `commit` command in a configuration script after specifying an IPv6 hardware ACL filter ensures that it is updated in the hardware.

**Example**  To update the hardware with the IPv6 ACL filter configuration, use the command:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-ipv6-acl
awplus(config-ipv6-hw-acl)# commit
```

**Related Commands**  ipv6 access-list (named)
ipv6 access-list (named)

**Overview**
Use this command to either create a new IPv6 hardware access-list, or to select an existing IPv6 hardware access-list in order to apply a filter entry to it.

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>
```

**Mode**
Global Configuration

**Default**
Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage**
Use IPv6 hardware named access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 hardware named access-list when a match is encountered.

For backwards compatibility you can either create IPv6 hardware named access-lists from within this command, or you can enter `ipv6 access-list` followed by only the IPv6 hardware named access-list name. This latter (and preferred) method moves you to the `(config-ipv6-hw-acl)` prompt for the selected IPv6 hardware named access-list number, and from here you can configure the filters for this selected IPv6 hardware named access-list.

*NOTE:* Hardware ACLs will permit access unless explicitly denied by an ACL action.

**Examples**
To create an IPv6 access-list named `my-ipv6-acl`, use the commands:
```
awplus# configure terminal
awplus(config)# ipv6 access-list my-ipv6-acl
awplus(config-ipv6-hw-acl)#
```

To delete the IPv6 access-list named `my-ipv6-acl`, use the commands:
```
awplus# configure terminal
awplus(config)# no ipv6 access-list my-ipv6-acl
```

**Validation Commands**
`show ipv6 access-list (IPv6 Hardware ACLs)`
**Related Commands**

- (ipv6 access-list named ICMP filter)
- (ipv6 access-list named protocol filter)
- (ipv6 access-list named TCP UDP filter)
- ipv6 traffic-filter
- show ipv6 access-list (IPv6 Hardware ACLs)
(ipv6 access-list named ICMP filter)

**Overview**  
Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with ICMP (Internet Control Message Protocol) packets, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

Note that specifying the `send-to-cpu` parameter could result in EPSR healthcheck messages and other control packets being dropped.

As an optional parameter `vlan` can be matched for tagged (802.1q) packet.

The `no` variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with ICMP (Internet Control Message Protocol) packets, from the current named IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

**NOTE:** Hardware ACLs will permit access unless explicitly denied by an ACL action.

**Syntax [ip|icmp]**

```plaintext
[<sequence-number>] {deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|copy-to-mirror} [ipv6] [icmp]  
{<ipv6-source-address/prefix-length>|<ipv6-source-address> <ipv6-source-wildcard>|host <ipv6-source-host>|any}  
{<ipv6-destination-address/prefix-length>|<ipv6-destination-address> <ipv6-destination-wildcard>|host <ipv6-destination-host-address>|any} [<icmp-type>] [vlan <1-4094>]  

no [
[<sequence-number>] {deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|copy-to-mirror} [ip|icmp]|{<ipv6-source-address/prefix-length>|<ipv6-source-address> <ipv6-source-wildcard>|host <ipv6-source-host>|any}  
{<ipv6-destination-address/prefix-length>|<ipv6-destination-address> <ipv6-destination-wildcard>|host <ipv6-destination-host-address>|any} [<icmp-type>] [vlan <1-4094>]  

no [<sequence-number>]}
```

**Parameter**  
**Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;sequence-number&gt;</code></td>
<td><code>&lt;1-65535&gt;</code>: The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies the packets to reject.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies the packets to permit.</td>
</tr>
</tbody>
</table>
### IPv6 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS

#### (IPv6 ACCESS-LIST NAMED ICMP FILTER)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>send-to-cpu</code></td>
<td>Specifies the packets to send to the CPU. Specifying this parameter could result in EPSR healthcheck messages and other control packets being dropped.</td>
</tr>
<tr>
<td><code>send-to-mirror</code></td>
<td>Specifies the packets to send to mirror port.</td>
</tr>
<tr>
<td><code>copy-to-cpu</code></td>
<td>Specifies the packets to copy to the CPU.</td>
</tr>
<tr>
<td><code>copy-to-mirror</code></td>
<td>Specifies the packets to copy to the mirror port.</td>
</tr>
<tr>
<td><code>ipv6</code></td>
<td>IPv6 packet, defined by the following parameters.</td>
</tr>
<tr>
<td><code>icmp</code></td>
<td>ICMP packet, defined by the following parameters.</td>
</tr>
<tr>
<td><code>&lt;ipv6-source-address/prefix-length&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;ipv6-source-address&gt;</code></td>
<td>Specifies the IPv6 source address. The IPv6 address uses the format X:X::X.</td>
</tr>
<tr>
<td><code>&lt;ipv6-source-wildcard&gt;</code></td>
<td>Specifies source wildcard bits in IPv6 format X:X::X. Note that binary 1 represents a don't care condition, and binary 0 represents a match.</td>
</tr>
<tr>
<td><code>host &lt;ipv6-source-host&gt;</code></td>
<td>Specifies a single source host address. The IPv6 address uses the format X:X::X.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies any Source host.</td>
</tr>
<tr>
<td><code>&lt;ipv6-destination-address/prefix-length&gt;</code></td>
<td>Specifies a destination address and prefix length. The IPv6 address uses the format X:X::X/Prefix-Length. The prefix-length is usually set between 0 and 64.</td>
</tr>
<tr>
<td><code>&lt;ipv6-destination-address&gt;</code></td>
<td>Specifies a destination address. The IPv6 address uses the format X:X::X.</td>
</tr>
<tr>
<td><code>&lt;ipv6-destination-wildcard&gt;</code></td>
<td>Specify destination wildcard bits in IPv6 format X:X::X.</td>
</tr>
<tr>
<td><code>host &lt;ipv6-destination-host-address&gt;</code></td>
<td>Specify a single destination host address. The IPv6 address uses the format X:X::X.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies any destination host.</td>
</tr>
<tr>
<td><code>&lt;icmp-type&gt;</code></td>
<td>Optional. Specify to filter by ICMP message type number. Valid values are from 0 to 255.</td>
</tr>
</tbody>
</table>
### IPV6 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS

#### (IPV6 ACCESS-LIST NAMED ICMP FILTER)

**Mode**
IPv6 Hardware ACL Configuration

**Default**
Any traffic on an interface controlled by a hardware ACL that does not explicate match a filter is permitted.

**Examples**
To specify a hardware IPv6 access-list named `my-acl1` and add an ACL filter entry that blocks all ICMP6 echo requests, enter the commands:

```plaintext
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl1
awplus(config-ipv6-hw-acl)# deny icmp any any icmp-type 128
```

To specify a hardware IPv6 access-list named `my-acl2` and add an ACL filter entry that blocks all ICMP6 echo requests on the default VLAN (`vlan1`), enter the following commands:

```plaintext
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl2
awplus(config-ipv6-hw-acl)# deny icmp any any icmp-type 128 vlan 1
```

To remove an ACL filter entry that blocks all ICMP6 echo requests from the hardware IPv6 access-list named `my-acl1`, enter the following commands:

```plaintext
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl1
awplus(config-ipv6-hw-acl)# no deny icmp any any icmp-type 128
```

**Validation Commands**
`show ipv6 access-list (IPv6 Hardware ACLs)`

**Related Commands**
- `ipv6 access-list (named)`
- `(ipv6 access-list named protocol filter)`
- `(ipv6 access-list named TCP UDP filter)`
- `ipv6 traffic-filter`
- `show ipv6 access-list (IPv6 Hardware ACLs)`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan</code></td>
<td>This parameter can be used in either single or double-tagged VLAN networks. It is the conventional VLAN tag (VID). In a double-tagged network it is sometimes referred to as the STAG.</td>
</tr>
<tr>
<td><code>&lt;1-4094&gt;</code></td>
<td>The VLAN VID.</td>
</tr>
</tbody>
</table>
Overview
Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with an IP protocol type specified, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

Note that specifying the `send-to-cpu` parameter could result in EPSR healthcheck messages and other control packets being dropped.

The `no` variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with an IP protocol type specified, from the current named IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

Syntax
```
[<sequence-number>]
{deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|copy-to-mirror} {ipv6|proto <ip-protocol>}
{<ipv6-source-prefix/prefix-length>|<ipv6-source-address>|ipv6-source-wildcard|host <ipv6-source-host>|any}
{<ipv6-destination-prefix/prefix-length>|<ipv6-destination-address>|ipv6-destination-wildcard|host <ipv6-destination-host>|any}
```

```
[<sequence-number>]
{deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|copy-to-mirror} {ipv6|proto <ip-protocol>}
{<ipv6-source-prefix/prefix-length>|<ipv6-source-address>|ipv6-source-wildcard|host <ipv6-source-host>|any}
{<ipv6-destination-prefix/prefix-length>|<ipv6-destination-address>|ipv6-destination-wildcard|host <ipv6-destination-host>|any}
```

```
no [<sequence-number>]
```

Parameter | Description
---|---
`<sequence-number>` | The sequence number for the filter entry of the selected access control list.
deny | Specifies packets to reject.
permit | Specifies packets to permit.
send-to-cpu | Specifies packets to send to the CPU. Specifying this parameter could result in EPSR healthcheck messages and other control packets being dropped.
send-to-mirror | Specifies packets to send to mirror port.
copy-to-cpu | Specifies packets to copy to the CPU.
copy-to-mirror | Specifies packets to copy to the mirror port.
ipv6 | Specifies IPv6 packet.
### IPv6 Hardware Access Control List (ACL) Commands

#### IPV6 ACCESS-LIST NAMED PROTOCOL FILTER

| Parameter       | Description                                                                述べ
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>proto &lt;ip-protocol&gt;</code></td>
<td>Specify IP protocol number &lt;1-255&gt;.</td>
</tr>
<tr>
<td><code>&lt;ip-protocol&gt;</code></td>
<td>The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority [<a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a>])</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol Number</th>
<th>Protocol Description [RFC Reference]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet Control Message [RFC792]</td>
</tr>
<tr>
<td>2</td>
<td>Internet Group Management [RFC1112]</td>
</tr>
<tr>
<td>3</td>
<td>Gateway-to-Gateway [RFC823]</td>
</tr>
<tr>
<td>4</td>
<td>IP in IP [RFC2003]</td>
</tr>
<tr>
<td>5</td>
<td>Stream [RFC1190] [RFC1819]</td>
</tr>
<tr>
<td>6</td>
<td>TCP (Transmission Control Protocol) [RFC793]</td>
</tr>
<tr>
<td>8</td>
<td>EGP (Exterior Gateway Protocol) [RFC888]</td>
</tr>
<tr>
<td>9</td>
<td>IGP (Interior Gateway Protocol) [IANA]</td>
</tr>
<tr>
<td>11</td>
<td>Network Voice Protocol [RFC741]</td>
</tr>
<tr>
<td>17</td>
<td>UDP (User Datagram Protocol) [RFC768]</td>
</tr>
<tr>
<td>20</td>
<td>Host monitoring [RFC869]</td>
</tr>
<tr>
<td>27</td>
<td>RDP (Reliable Data Protocol) [RFC908]</td>
</tr>
<tr>
<td>28</td>
<td>IRTP (Internet Reliable Transaction Protocol) [RFC938]</td>
</tr>
<tr>
<td>29</td>
<td>ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]</td>
</tr>
<tr>
<td>30</td>
<td>Bulk Data Transfer Protocol [RFC969]</td>
</tr>
<tr>
<td>33</td>
<td>DCCP (Datagram Congestion Control Protocol) [RFC4340]</td>
</tr>
<tr>
<td>48</td>
<td>DSR (Dynamic Source Routing Protocol) [RFC4728]</td>
</tr>
<tr>
<td>50</td>
<td>ESP (Encap Security Payload) [RFC2406]</td>
</tr>
<tr>
<td>51</td>
<td>AH (Authentication Header) [RFC2402]</td>
</tr>
<tr>
<td>54</td>
<td>NARP (NBMA Address Resolution Protocol) [RFC1735]</td>
</tr>
<tr>
<td>58</td>
<td>ICMP for IPv6 [RFC1883]</td>
</tr>
<tr>
<td>59</td>
<td>No Next Header for IPv6 [RFC1883]</td>
</tr>
<tr>
<td>60</td>
<td>Destination Options for IPv6 [RFC1883]</td>
</tr>
<tr>
<td>88</td>
<td>EIGRP (Enhanced Interior Gateway Routing Protocol)</td>
</tr>
<tr>
<td>89</td>
<td>OSPFIGP [RFC1583]</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-protocol&gt;</code> (cont.)</td>
<td>97   Ethernet-within-IP Encapsulation / RFC3378</td>
</tr>
<tr>
<td></td>
<td>98   Encapsulation Header / RFC1241</td>
</tr>
<tr>
<td></td>
<td>108  IP Payload Compression Protocol / RFC2393</td>
</tr>
<tr>
<td></td>
<td>112  Virtual Router Redundancy Protocol / RFC3768</td>
</tr>
<tr>
<td></td>
<td>134  RSVP-E2E-IGNORE / RFC3175</td>
</tr>
<tr>
<td></td>
<td>135  Mobility Header / RFC3775</td>
</tr>
<tr>
<td></td>
<td>136  UDPLite / RFC3828</td>
</tr>
<tr>
<td></td>
<td>137  MPLS-in-IP / RFC4023</td>
</tr>
<tr>
<td></td>
<td>138  MANET Protocols / RFC-ietf-manet-iana-07.txt</td>
</tr>
<tr>
<td></td>
<td>139-252 Unassigned / IANA</td>
</tr>
<tr>
<td></td>
<td>253  Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td></td>
<td>254  Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td></td>
<td>255  Reserved / IANA</td>
</tr>
<tr>
<td><code>&lt;ipv6-source-prefix/prefix-length&gt;</code></td>
<td>Specify source address and mask.</td>
</tr>
<tr>
<td></td>
<td>The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.</td>
</tr>
<tr>
<td><code>&lt;ipv6-source-address&gt;</code></td>
<td>Specifies the source address.</td>
</tr>
<tr>
<td></td>
<td>The IPv6 address uses the format X:X::X.</td>
</tr>
<tr>
<td><code>&lt;ipv6-source-wildcard&gt;</code></td>
<td>Specifies the source wildcard bits, in IPv6 format X:X::X.</td>
</tr>
<tr>
<td><code>host &lt;ipv6-source-host&gt;</code></td>
<td>Specifies a single source host.</td>
</tr>
<tr>
<td></td>
<td>The IPv6 address uses the format X:X::X.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies any source host.</td>
</tr>
<tr>
<td></td>
<td>An abbreviation for the IPv6 prefix ::/0</td>
</tr>
<tr>
<td><code>&lt;ipv6-dest-prefix/prefix-length&gt;</code></td>
<td>Specifies a destination address and mask.</td>
</tr>
<tr>
<td></td>
<td>The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.</td>
</tr>
<tr>
<td><code>&lt;ipv6-destination-address&gt;</code></td>
<td>Specify destination address.</td>
</tr>
<tr>
<td></td>
<td>The IPv6 address uses the format X:X::X.</td>
</tr>
<tr>
<td><code>&lt;ipv6-destination-wildcard&gt;</code></td>
<td>Specify destination wildcard bits in IPv6 format X:X::X</td>
</tr>
<tr>
<td><code>host &lt;ipv6-destination-host&gt;</code></td>
<td>Specify a single destination host address.</td>
</tr>
<tr>
<td></td>
<td>The IPv6 address uses the format X:X::X.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies any destination host.</td>
</tr>
<tr>
<td></td>
<td>An abbreviation for the IPv6 prefix ::/0</td>
</tr>
<tr>
<td><code>vlan</code></td>
<td>This parameter can be used in either single or double-tagged VLAN networks. It is the conventional VLAN tag (VID). In a double-tagged network it is sometimes referred to as the STAG.</td>
</tr>
<tr>
<td><code>&lt;1-4094&gt;</code></td>
<td>The VLAN VID.</td>
</tr>
</tbody>
</table>
**Mode**  IPv6 Hardware ACL Configuration

**Default**  Any traffic on an interface controlled by a hardware ACL that does not explicate match a filter is permitted.

**Usage**  This command adds a hardware classification filter (for use with features such as QoS), to a current standard IPv6 access-list. The filter will match on any IP protocol type packet that has the specified source and destination IPv6 addresses and the specified IP protocol type. The parameter any may be specified if an address does not matter,

*NOTE:* Hardware ACLs will permit access unless explicitly denied by an ACL action.

**Examples**  To add an ACL filter entry to block IP traffic from network 2001:0db8::0/64 to the hardware IPv6 access-list named my-acl, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny ipv6 2001:0db8::0/64
```

To remove an ACL filter entry that blocks all IPv6 traffic from network 2001:0db8::0/64 from the hardware IPv6 access-list named my-acl, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# no deny ipv6 2001:0db8::0/64
```

**Validation Commands**  show ipv6 access-list (IPv6 Hardware ACLs)

**Related Commands**  ipv6 access-list (named)
(ipv6 access-list named ICMP filter)
(ipv6 access-list named TCP UDP filter)
ipv6 traffic-filter
show ipv6 access-list (IPv6 Hardware ACLs)
(ipv6 access-list named TCP UDP filter)

**Overview**  
Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) source and destination ports specified, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

Note that specifying the `send-to-cpu` parameter could result in EPSR healthcheck messages and other control packets being dropped.

The `no` variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with TCP or UDP source and destination ports specified, from the current named IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

**Syntax**

```
[<sequence-number>] {deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|copy-to-mirror|tcp|udp}
{<ipv6-source-prefix/prefix-length>|<ipv6-source-address>
<ipv6-source-wildcard>|host <ipv6-source-host>|any} {eq <sourceport>|lt <sourceport>|gt <sourceport>|ne <sourceport>}|[range <start-range><end-range>]
{<ipv6-destination-prefix/prefix-length>|<ipv6-destination-address>
<ipv6-destination-wildcard>|host <ipv6-destination-host>|any} {eq <destport>|lt <destport>|gt <destport>|ne <destport>}|[range <start-range><end-range>]
no {deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|copy-to-mirror|tcp|udp}
{<ipv6-source-prefix/prefix-length>|<ipv6-source-address>
<ipv6-source-wildcard>|host <ipv6-source-host>|any} {eq <sourceport>|lt <sourceport>|gt <sourceport>|ne <sourceport>}|[range <start-range><end-range>]
{<ipv6-destination-prefix/prefix-length>|<ipv6-destination-address>
<ipv6-destination-wildcard>|host <ipv6-destination-host>|any} {eq <destport>|lt <destport>|gt <destport>|ne <destport>}|[range <start-range><end-range>]
no <sequence-number>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;sequence-number&gt;</code></td>
<td><code>&lt;1-65535&gt;</code> The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Specify packets to reject.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies the packets to permit.</td>
</tr>
</tbody>
</table>

---

**Parameter**

- `<sequence-number>`
- `deny`
- `permit`
### IPv6 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS

**IPv6 ACCESS-LIST NAMED TCP UDP FILTER**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>send-to-cpu</td>
<td>Specifies the packets to send to the CPU. Specifying this parameter could result in EPSR healthcheck messages and other control packets being dropped.</td>
</tr>
<tr>
<td>send-to-mirror</td>
<td>Specifies the packets to send to mirror port.</td>
</tr>
<tr>
<td>copy-to-cpu</td>
<td>Specifies the packets to copy to the CPU.</td>
</tr>
<tr>
<td>copy-to-mirror</td>
<td>Specifies the packets to copy to the mirror port.</td>
</tr>
<tr>
<td>tcp</td>
<td>Specifies a TCP packet.</td>
</tr>
<tr>
<td>udp</td>
<td>Specifies a UDP packet.</td>
</tr>
<tr>
<td>&lt;ipv6-source-prefix/</td>
<td>Specifies the source address with mask. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.</td>
</tr>
<tr>
<td>prefix-length&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;ipv6-source-address&gt;</td>
<td>Specifies the source address. The IPv6 address uses the format X:X::X:X.</td>
</tr>
<tr>
<td>&lt;ipv6-source-wildcard&gt;</td>
<td>Specifies the source wildcard bits in IPv6 format X:X::X:X.</td>
</tr>
<tr>
<td>host &lt;ipv6-source-host&gt;</td>
<td>Specifies the a single source host. The IPv6 address uses the format X:X::X:X.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies any Source host. An abbreviation for the IPv6 prefix ::/0.</td>
</tr>
<tr>
<td>eq</td>
<td>Equal to.</td>
</tr>
<tr>
<td>lt</td>
<td>Less than.</td>
</tr>
<tr>
<td>gt</td>
<td>Greater than.</td>
</tr>
<tr>
<td>ne</td>
<td>Not equal to.</td>
</tr>
<tr>
<td>&lt;sourceport&gt;</td>
<td>The source port number, specified as an integer between 0 and 65535.</td>
</tr>
<tr>
<td>&lt;destport&gt;</td>
<td>The destination port number, specified as an integer between 0 and 65535.</td>
</tr>
<tr>
<td>range</td>
<td>Range of port numbers. Match only packets within range.</td>
</tr>
<tr>
<td>&lt;start-range&gt;</td>
<td>The port number at the start of the range &lt;0-65535&gt;.</td>
</tr>
<tr>
<td>&lt;end-range&gt;</td>
<td>The port number at the end of the range &lt;0-65535&gt;.</td>
</tr>
<tr>
<td>&lt;ipv6-dest-prefix/</td>
<td>Specify destination address with mask. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.</td>
</tr>
<tr>
<td>prefix-length&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;ipv6-destination-</td>
<td>Specify destination address. The IPv6 address uses the format X:X::X:X.</td>
</tr>
<tr>
<td>address&gt;</td>
<td></td>
</tr>
</tbody>
</table>
**Mode**  
IPv6 Hardware ACL Configuration

**Default**  
Any traffic on an interface controlled by a hardware ACL that does not explicate match a filter is permitted.

**Usage**  
The filter entry will match on any TCP or UDP packet that has the specified source and destination IPv6 addresses and TCP or UDP type. The parameter any may be specified if an address does not matter.

**NOTE:** Hardware ACLs will permit access unless explicitly denied by an ACL action.

**Examples**  
To add an ACL filter entry that blocks all SSH traffic from network 2001:0db8::0/64 to the hardware IPv6 access-list named my-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 an ACL 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
```

**Validation Commands**

```
show ipv6 access-list (IPv6 Hardware ACLs)
```
IPV6 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS
(IPV6 ACCESS-LIST NAMED TCP UDP FILTER)

Related Commands

ipv6 access-list (named)
(ipv6 access-list named ICMP filter)
(ipv6 access-list named protocol filter)
ipv6 traffic-filter
show ipv6 access-list (IPv6 Hardware ACLs)
IPV6 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS

IPV6 TRAFFIC-FILTER

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>

Mode
Interface Configuration (to apply an IPv6 hardware ACL to a specific switch port).

Usage
This command adds an IPv6 hardware-based access-list to an interface. The number of access-lists that can be added is determined by the amount of available space in the hardware-based packet classification tables.

To apply the access-list to all ports on the switch, execute the command in the Global Configuration mode. To apply the access-list to a Layer 2 interface or Layer 2 interface range, apply the command in the Interface Configuration mode. See the examples for each mode below.

Examples
To add access-list acl1 as a traffic-filter to interface port1.0.1, enter the commands:

awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# ipv6 traffic-filter acl1

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

Parameter | Description
--- | ---
<ipv6-access-list-name> | Hardware IPv6 access-list name.

**Related Commands**

- `ipv6 access-list (named)`
- `(ipv6 access-list named ICMP filter)`
- `(ipv6 access-list named protocol filter)`
- `(ipv6 access-list named TCP UDP filter)`
- `ipv6 traffic-filter`
- `show ipv6 access-list (IPv6 Hardware ACLs)`
show ipv6 access-list (IPv6 Hardware ACLs)

**Overview**  Use this command to display all configured hardware IPv6 access-lists or the IPv6 access-list specified by name. Omitting the optional access-list name parameter will display all IPv6 ACLs.

Use the `show ipv6 access-list standard` command to display the IPv6 access-list specified by name as defined from the `ipv6 access-list (named)` command.

**Syntax**  
`show ipv6 access-list [access-list-name]`

`show ipv6 access-list standard [access-list-name]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>standard</td>
<td>Named standard access-list.</td>
</tr>
<tr>
<td>&lt;access-list-name&gt;</td>
<td>Hardware IPv6 access-list name.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Examples**  To show the standard named ipv6 access-list acl_name use the following command:

```
awplus# show ipv6 access-list standard acl_name
```

**Output**  Figure 32-1:  Example output from the `show ipv6 access-list standard` command

```
Named Standard IPv6 access-list acl_name
  deny any
```

To show all configured ipv6 access-lists use the command:

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

**Output**  Figure 32-2:  Example output from the `show ipv6 access-list` command

```
IPv6 access-list deny_icmp
  deny icmp any any vlan 1

IPv6 access-list deny_ssh
  deny tcp abcd::/64 any eq 22
```
IPV6 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS
SHOW IPV6 ACCESS-LIST (IPV6 HARDWARE ACLs)

Related Commands

ipv6 access-list (named)
(ipv6 access-list named ICMP filter)
(ipv6 access-list named protocol filter)
(ipv6 access-list named TCP UDP filter)
ipv6 traffic-filter
IPV6 HARDWARE ACCESS CONTROL LIST (ACL) COMMANDS
SHOW IPV6 ACCESS-LIST (IPV6 HARDWARE ACLs)
Introduction

Overview
This chapter provides an alphabetical reference for the IPv6 Software Access Control List (ACL) commands, and contains detailed command information and command examples about IPv6 software ACLs as applied to Routing and Multicasting, which are not applied to interfaces.

For information about ACLs, see the ACL Feature Overview and Configuration Guide.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see the following references:

- the Link Aggregation Feature Overview and Configuration Guide.
- Link Aggregation Commands

Note that text in parenthesis in command names indicates usage not keyword entry. For example, `ipv6-access-list (named)` indicates named IPv6 ACLs entered as `ipv6-access-list <name>` where `<name>` is a placeholder not a keyword.

Note also that parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI. For example, `(ipv6 access-list standard IPv6 filter)` represents command entry in the format:

`[<sequence-number>] [deny|permit] [<IPv6-source-address/prefix-length>|any].`

**NOTE:** Software ACLs will *deny* access unless *explicitly permitted* by an ACL action.

Sub-modes
Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.
### Table 33-1: IPv6 Software Access List Commands and Prompts

<table>
<thead>
<tr>
<th>Command Name</th>
<th>Command Mode</th>
<th>Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 access-list (IPv6 Software ACLs)</td>
<td>Privileged Exec</td>
<td>awplus#</td>
</tr>
<tr>
<td>ipv6 access-list extended (named)</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>ipv6 access-list standard (named)</td>
<td>Global Configuration</td>
<td>awplus(config)#</td>
</tr>
<tr>
<td>(ipv6 access-list extended IP protocol filter)</td>
<td>IPv6 Extended ACL</td>
<td>awplus(config-ipv6-ext-acl)#</td>
</tr>
<tr>
<td>(ipv6 access-list extended TCP UDP filter)</td>
<td>IPv6 Extended ACL</td>
<td>awplus(config-ipv6-ext-acl)#</td>
</tr>
<tr>
<td>(ipv6 access-list standard filter)</td>
<td>IPv6 Standard ACL</td>
<td>awplus(config-ipv6-std-acl)#</td>
</tr>
</tbody>
</table>

**Command List**

- “ipv6 access-list extended (named)” on page 1403
- “ipv6 access-list extended proto” on page 1407
- “(ipv6 access-list extended IP protocol filter)” on page 1410
- “(ipv6 access-list extended TCP UDP filter)” on page 1413
- “ipv6 access-list standard (named)” on page 1415
- “(ipv6 access-list standard filter)” on page 1417
- “ipv6 prefix-list” on page 1419
- “show ipv6 access-list (IPv6 Software ACLs)” on page 1421
- “show ipv6 prefix-list” on page 1422
IPV6 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS
IPV6 ACCESS-LIST EXTENDED (NAMED)

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
ipv6 access-list extended <list-name>
no ipv6 access-list extended <list-name>

Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;list-name&gt;</td>
<td>A user-defined name for the IPv6 software extended access-list.</td>
</tr>
</tbody>
</table>

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>|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>|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>} {eq <destport>|lt <destport>|gt <destport>|ne <destport>} {any} [{<icmp-type>|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>} {eq <destport>|lt <destport>|gt <destport>|ne <destport>} {any} [{<icmp-type>|log}]

Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;list-name&gt;</td>
<td>A user-defined name for the IPv6 software extended access-list.</td>
</tr>
<tr>
<td>deny</td>
<td>The IPv6 software extended access-list rejects packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>The IPv6 software extended access-list permits packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
</tbody>
</table>
| any | For ICMP|IP
The IPv6 software extended access-list matches any type of packet. |
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
**IPV6 ACCESS-LIST EXTENDED (NAMED)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;icmp-type&gt;</code></td>
<td>For ICMP</td>
</tr>
<tr>
<td>0</td>
<td>Echo replies.</td>
</tr>
<tr>
<td>3</td>
<td>Destination unreachable messages.</td>
</tr>
<tr>
<td>4</td>
<td>Source quench messages.</td>
</tr>
<tr>
<td>5</td>
<td>Redirect (change route) messages.</td>
</tr>
<tr>
<td>8</td>
<td>Echo requests.</td>
</tr>
<tr>
<td>11</td>
<td>Time exceeded messages.</td>
</tr>
<tr>
<td>12</td>
<td>Parameter problem messages.</td>
</tr>
<tr>
<td>13</td>
<td>Timestamp requests.</td>
</tr>
<tr>
<td>14</td>
<td>Timestamp replies.</td>
</tr>
<tr>
<td>15</td>
<td>Information requests.</td>
</tr>
<tr>
<td>16</td>
<td>Information replies.</td>
</tr>
<tr>
<td>17</td>
<td>Address mask requests.</td>
</tr>
<tr>
<td>18</td>
<td>Address mask replies.</td>
</tr>
</tbody>
</table>

| 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**  
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:

```bash
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:

```bash
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:

```bash
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` (ipv6 access-list extended TCP UDP filter)
- `show ipv6 access-list (IPv6 Software ACLs)`
- `show running-config`
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> \n{<ipv6-source-address/prefix>|any} \n{<ipv6-destination-address/prefix>|any} [log]
```
```
no ipv6 access-list extended <list-name> {deny|permit} proto <ip-protocol> \n{<ipv6-source-address/prefix>|any} \n{<ipv6-destination-address/prefix>|any} [log]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;list-name&gt;</code></td>
<td>A user-defined name for the IPv6 software extended access-list.</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>Specifies the packets to reject.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Specifies the packets to accept.</td>
</tr>
<tr>
<td><code>proto</code></td>
<td>The IP Protocol type specified by it protocol number <code>&lt;1-255&gt;</code>.</td>
</tr>
<tr>
<td><code>&lt;ip-protocol&gt;</code></td>
<td>The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority) [<a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a>]</td>
</tr>
</tbody>
</table>

**Protocol Number** | **Protocol Description** | **RFC Reference** |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet Control Message</td>
<td>[RFC792]</td>
</tr>
<tr>
<td>2</td>
<td>Internet Group Management</td>
<td>[RFC1112]</td>
</tr>
<tr>
<td>3</td>
<td>Gateway-to-Gateway [RFC823]</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>IP in IP [RFC2003]</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Stream [RFC1190] [RFC1819]</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>TCP (Transmission Control Protocol) [RFC793]</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>EGP (Exterior Gateway Protocol) [RFC888]</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>IGP (Interior Gateway Protocol) [IANA]</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Network Voice Protocol [RFC741]</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>UDP (User Datagram Protocol) [RFC768]</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Host monitoring [RFC869]</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>RDP (Reliable Data Protocol) [RFC908]</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>IRTP (Internet Reliable Transaction Protocol) [RFC938]</td>
<td></td>
</tr>
</tbody>
</table>
### IPV6 ACCESS-LIST EXTENDED PROTO

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]</td>
</tr>
<tr>
<td>30</td>
<td>Bulk Data Transfer Protocol [RFC969]</td>
</tr>
<tr>
<td>33</td>
<td>DCCP (Datagram Congestion Control Protocol) [RFC4340]</td>
</tr>
<tr>
<td>48</td>
<td>DSR (Dynamic Source Routing Protocol) [RFC4728]</td>
</tr>
<tr>
<td>50</td>
<td>ESP (Encap Security Payload) [RFC2406]</td>
</tr>
<tr>
<td>51</td>
<td>AH (Authentication Header) [RFC2402]</td>
</tr>
<tr>
<td>54</td>
<td>NARP (NBMA Address Resolution Protocol) [RFC1735]</td>
</tr>
<tr>
<td>58</td>
<td>ICMP for IPv6 [RFC1883]</td>
</tr>
<tr>
<td>59</td>
<td>No Next Header for IPv6 [RFC1883]</td>
</tr>
<tr>
<td>60</td>
<td>Destination Options for IPv6 [RFC1883]</td>
</tr>
<tr>
<td>88</td>
<td>EIGRP (Enhanced Interior Gateway Routing Protocol)</td>
</tr>
<tr>
<td>89</td>
<td>OSPF [RFC1583]</td>
</tr>
<tr>
<td>97</td>
<td>Ethernet-within-IP Encapsulation / RFC3378</td>
</tr>
<tr>
<td>98</td>
<td>Encapsulation Header / RFC1241</td>
</tr>
<tr>
<td>108</td>
<td>IP Payload Compression Protocol / RFC2393</td>
</tr>
<tr>
<td>112</td>
<td>Virtual Router Redundancy Protocol / RFC3768</td>
</tr>
<tr>
<td>134</td>
<td>RSVP-E2E-IGNORE / RFC3175</td>
</tr>
<tr>
<td>135</td>
<td>Mobility Header / RFC3775</td>
</tr>
<tr>
<td>136</td>
<td>UDPLite / RFC3828</td>
</tr>
<tr>
<td>137</td>
<td>MPLS-in-IP / RFC4023</td>
</tr>
<tr>
<td>138</td>
<td>MANET Protocols / RFC-ietf-manet-iana-07.txt</td>
</tr>
<tr>
<td>139–252</td>
<td>Unassigned / IANA</td>
</tr>
<tr>
<td>253</td>
<td>Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td>254</td>
<td>Use for experimentation and testing / RFC3692</td>
</tr>
<tr>
<td>255</td>
<td>Reserved / IANA</td>
</tr>
</tbody>
</table>

<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 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS

IPV6 ACCESS-LIST EXTENDED PROTO

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipv6-destination-address/prefix&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>any</td>
<td>Any destination address or remote address.</td>
</tr>
<tr>
<td>log</td>
<td>Log the results.</td>
</tr>
</tbody>
</table>

**Mode**  
Global Configuration

**Default**  
Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage**  
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 9 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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;sequence-number&gt;</code></td>
<td><code>&lt;1-65535&gt;</code> The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies the packets to reject.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies the packets to accept.</td>
</tr>
<tr>
<td>ip</td>
<td>IP packet.</td>
</tr>
<tr>
<td>any</td>
<td>Any packet.</td>
</tr>
<tr>
<td>proto <code>&lt;ip-protocol&gt;</code></td>
<td>The IP Protocol type specified by it protocol number <code>&lt;1-255&gt;</code>.</td>
</tr>
<tr>
<td><code>&lt;ip-protocol&gt;</code></td>
<td>The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority <a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a>).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>8</td>
</tr>
</tbody>
</table>
### IPV6 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS

(IPv6 ACCESS-LIST EXTENDED IP PROTOCOL FILTER)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-protocol&gt;</code> (cont.)</td>
<td>Protocol Number 9</td>
</tr>
<tr>
<td>11</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td></td>
</tr>
<tr>
<td>58</td>
<td></td>
</tr>
<tr>
<td>59</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td></td>
</tr>
<tr>
<td>88</td>
<td></td>
</tr>
<tr>
<td>89</td>
<td></td>
</tr>
<tr>
<td>97</td>
<td></td>
</tr>
<tr>
<td>98</td>
<td></td>
</tr>
<tr>
<td>108</td>
<td></td>
</tr>
<tr>
<td>112</td>
<td></td>
</tr>
<tr>
<td>134</td>
<td></td>
</tr>
<tr>
<td>135</td>
<td></td>
</tr>
<tr>
<td>136</td>
<td></td>
</tr>
<tr>
<td>137</td>
<td></td>
</tr>
<tr>
<td>138</td>
<td></td>
</tr>
<tr>
<td>139-252</td>
<td>IPv6 source address, or local address. The IPv6 address uses the format X::X::X/Prefix-Length. The prefix-length is usually set between 0 and 64.</td>
</tr>
<tr>
<td>253</td>
<td></td>
</tr>
<tr>
<td>254</td>
<td></td>
</tr>
<tr>
<td>255</td>
<td></td>
</tr>
<tr>
<td><code>ipv6-source-address/prefix</code></td>
<td>Any source address or local address.</td>
</tr>
</tbody>
</table>
IPV6 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS
(IPV6 ACCESS-LIST EXTENDED IP PROTOCOL FILTER)

**Mode** IPv6 Extended 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 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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv6-destination-address/prefix&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Any destination address or remote address.</td>
</tr>
<tr>
<td><code>log</code></td>
<td>Log the results.</td>
</tr>
</tbody>
</table>
## (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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;sequence-number&gt;</td>
<td>The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies the packets to reject.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies the packets to accept.</td>
</tr>
<tr>
<td>tcp</td>
<td>TCP packet.</td>
</tr>
<tr>
<td>udp</td>
<td>UDP packet.</td>
</tr>
<tr>
<td>&lt;ipv6-source-address/prefix&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>any</td>
<td>Any source address or local address.</td>
</tr>
<tr>
<td>eq</td>
<td>Equal to.</td>
</tr>
<tr>
<td>lt</td>
<td>Less than.</td>
</tr>
<tr>
<td>gt</td>
<td>Greater than.</td>
</tr>
<tr>
<td>ne</td>
<td>Not equal to.</td>
</tr>
<tr>
<td>&lt;sourceport&gt;</td>
<td>The source port number, specified as an integer between 0 and 65535.</td>
</tr>
</tbody>
</table>
IPV6 SOFTWARE ACCESS CONTROL LIST (ACL) COMMANDS
(ipv6 access-list extended TCP UDP FILTER)

Mode
IPv6 Extended 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 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipv6-destination-address/prefix&gt;</td>
<td>IPv6 destination address, or local address. The IPv6 address uses the format XX::XX/Prefix-Length. The prefix-length is usually set between 0 and 64.</td>
</tr>
<tr>
<td>&lt;destport&gt;</td>
<td>The destination port number, specified as an integer between 0 and 65535.</td>
</tr>
<tr>
<td>log</td>
<td>Log the results.</td>
</tr>
</tbody>
</table>
**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**

```
ipv6 access-list standard <ipv6-acl-list-name>
no ipv6 access-list standard <ipv6-acl-list-name>
```

**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]]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv6-acl-list-name&gt;</code></td>
<td>A user-defined name for the IPv6 software standard access-list.</td>
</tr>
<tr>
<td>deny</td>
<td>The IPv6 software standard access-list rejects packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td>permit</td>
<td>The IPv6 software standard access-list permits packets that match the type, source, and destination filtering specified with this command.</td>
</tr>
<tr>
<td><code>&lt;ipv6-source-address/prefix-length&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td>any</td>
<td>Matches any source IPv6 address.</td>
</tr>
<tr>
<td>exact-match</td>
<td>Exact match of the prefixes.</td>
</tr>
</tbody>
</table>

**Mode**

Global Configuration

**Default**

Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage**

Use IPv6 standard access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 standard access-list when a match is encountered.
For backwards compatibility you can either create IPv6 standard access-lists from within this command, or you can enter `ipv6 access-list standard` followed by only the IPv6 standard access-list name. This latter (and preferred) method moves you to the `ipv6 access-list standard` 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`
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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;sequence-number&gt;</code></td>
<td>&lt;1-65535&gt; The sequence number for the filter entry of the selected access control list.</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies the packets to reject.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies the packets to accept.</td>
</tr>
<tr>
<td><code>&lt;ipv6-source-address/prefix-length&gt;</code></td>
<td>IPv6 source address and prefix-length in the form X:X::X:X/P.</td>
</tr>
<tr>
<td>any</td>
<td>Any IPv6 source host address.</td>
</tr>
</tbody>
</table>

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:

```bash
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:

```bash
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 or a prefix list entry.

**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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;list-name&gt;</td>
<td>Specifies the name of a prefix list.</td>
</tr>
<tr>
<td>seq &lt;1-429496725&gt;</td>
<td>Sequence number of the prefix list entry.</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies that the prefixes are excluded from the list.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies that the prefixes are included in the list.</td>
</tr>
<tr>
<td>&lt;ipv6-prefix&gt;</td>
<td>Specifies the IPv6 prefix and prefix length in hexadecimal in the format X:X::X:X/M.</td>
</tr>
<tr>
<td>any</td>
<td>Any prefix match. Same as ::0/0 le 128.</td>
</tr>
<tr>
<td>ge &lt;0-128&gt;</td>
<td>Specifies the minimum prefix length to be matched.</td>
</tr>
<tr>
<td>le &lt;0-128&gt;</td>
<td>Specifies the maximum prefix length to be matched.</td>
</tr>
<tr>
<td>description</td>
<td>Prefix list specific description.</td>
</tr>
<tr>
<td>&lt;text&gt;</td>
<td>Up to 80 characters of text description of the prefix list.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Usage**
When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the seq parameter and place common permits or denials towards the top of the list. If you do not use the seq parameter, the sequence values are generated in a sequence of 5.

The parameters ge and le specify the range of the prefix lengths to be matched. 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 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 the `show ipv6 access-list standard` command to display a specified standard named IPv6 access-list that has been defined using the `ipv6 access-list standard (named)` command.

**Syntax**
```
show ipv6 access-list standard <access-list-name>
```

**Mode**
User Exec and Privileged Exec

**Example**
To show the ipv6 access-list specified with the name `acl_name` use the following command:
```
awplus# show ipv6 access-list standard acl_name
```

**Output**
Figure 33-1: Example output from the show ipv6 access-list standard command
```
Named Standard IPv6 access-list name
deny any
```

**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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>Specify the name of an individual IPv6 prefix list.</td>
</tr>
<tr>
<td>detail</td>
<td>Specify this parameter to show detailed output for all IPv6 prefix lists.</td>
</tr>
<tr>
<td>summary</td>
<td>Specify this parameter to show summary output for all IPv6 prefix lists.</td>
</tr>
</tbody>
</table>

**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
Introduction

Overview

This chapter provides an alphabetical reference for Quality of Service commands. For more information, see the QoS Feature Overview and Configuration Guide and the ACL Feature Overview and Configuration Guide.
QoS COMMANDS

Command List

• “class” on page 1426
• “class-map” on page 1427
• “clear mls qos interface policer-counters” on page 1428
• “default-action” on page 1429
• “description (QoS policy-map)” on page 1430
• “egress-rate-limit” on page 1431
• “match access-group” on page 1432
• “match cos” on page 1434
• “match dscp” on page 1435
• “match eth-format protocol” on page 1436
• “match inner-cos” on page 1439
• “match inner-vlan” on page 1440
• “match ip-precedence” on page 1441
• “match mac-type” on page 1442
• “match tcp-flags” on page 1443
• “match vlan” on page 1444
• “mls qos cos” on page 1445
• “mls qos enable” on page 1446
• “mls qos map cos-queue to” on page 1447
• “mls qos map premark-dscp to” on page 1448
• “no police” on page 1450
• “police single-rate action” on page 1451
• “police twin-rate action” on page 1453
• “policy-map” on page 1455
• “priority-queue” on page 1456
• “remark-map” on page 1457
• “remark new-cos” on page 1459
• “service-policy input” on page 1461
• “set ip next-hop (PBR)” on page 1462
• “show class-map” on page 1463
• “show mls qos” on page 1464
• “show mls qos interface” on page 1465
• “show mls qos interface policer-counters” on page 1468
• “show mls qos interface queue-counters” on page 1470
• “show mls qos interface storm-status” on page 1471
QoS COMMANDS

- “show mls qos maps cos-queue” on page 1472
- “show mls qos maps premark-dscp” on page 1473
- “show policy-map” on page 1474
- “storm-action” on page 1475
- “storm-downtime” on page 1476
- “storm-protection” on page 1477
- “storm-rate” on page 1478
- “storm-window” on page 1479
- “trust dscp” on page 1480
- “wrr-queue disable queues” on page 1481
- “wrr-queue egress-rate-limit queues” on page 1482
- “wrr-queue weight queues” on page 1483
class

**Overview**  Use this command to associate an existing class-map to a policy or policy-map (traffic classification), and to enter Policy Map Class Configuration mode to configure the class-map.

Use the **no** variant of this command to delete an existing class-map.

For more information on class-maps and policy-maps, see the **QoS Feature Overview** and **Configuration Guide**.

If your class-map does not exist, you can create it by using the **class-map** command.

**Syntax**

```
class {<name>|default}
no class <name>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>Name of the (already existing) class-map.</td>
</tr>
<tr>
<td>default</td>
<td>Specify the default class-map.</td>
</tr>
</tbody>
</table>

**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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>Name of the class-map to be created.</td>
</tr>
</tbody>
</table>

**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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>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).</td>
</tr>
<tr>
<td>class-map</td>
<td>Select a class-map.</td>
</tr>
<tr>
<td>&lt;class-map&gt;</td>
<td>Class-map name.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
To reset the policy counters to zero for all class-maps for port1.0.1, use the command:
```
awplus# clear mls qos interface port1.0.1 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
[permit|deny|send-to-cpu|copy-to-cpu|copy-to-mirror|
send-to-mirror]
no default-action
```

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;line&gt;</td>
<td>Up to 80 character long line description.</td>
</tr>
</tbody>
</table>

**Mode**  Policy Map Configuration

**Example**  To add the description, VOIP traffic, use the command:
```
awplus(config-pmap)# description VOIP traffic
```
QoS Commands

Egress-rate-limit

**Overview**
Sets a limit on the amount of traffic that can be transmitted per second from this port.

Use the no variant of this command to disable the limiting of traffic egressing on the interface.

**Syntax**
```plaintext
egress-rate-limit <bandwidth>
no egress-rate-limit
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;bandwidth&gt;</td>
<td>Bandwidth &lt;1-10000000 units per second&gt; (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 taken as 20 megabits.</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration

**Examples**
To enable egress rate limiting on a port, use the commands:

```plaintext
awplus# configure terminal
aplus(config)# interface port1.0.1
awplus(config-if)# egress-rate-limit 64k
% Egress rate limit has been set to 64 Kb
```

To disable egress rate limiting on a port, use the commands:

```plaintext
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no egress-rate-limit
```
match access-group

**Overview**  Use this command to define match criterion for a class-map.

**Syntax**

```plaintext
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>}
```

**Mode**  Class Map Configuration

**Usage**  First create an access-list that applies the appropriate permit/deny requirements. Then use the **match access-group** command to apply this access-list for matching to a class-map. Note that this command will apply the access-list matching only to incoming data packets.

**Examples**

To configure a class-map named cmap1 with one match criterion: access-list 3001, which allows IP traffic from any source to any destination, use the commands:

```plaintext
awplus# configure terminal
awplus(config)# access-list 3001 permit ip any any
awplus(config)# class-map cmap1
awplus(config-cmap)# match access-group 3001
```

To configure a class-map named cmap2 with one match criterion: access-list 3001, which allows MAC traffic from any source to any destination, use the commands:

```plaintext
awplus# configure terminal
awplus(config)# access-list 4001 permit any any
awplus(config)# class-map cmap2
awplus(config-cmap)# match access-group 4001
```
To configure a class-map named cmap3 with one match criterion: access-list hw_acl, which allows IP traffic from any source to any destination, use the commands:

awplus# configure terminal
awplus(config)# access-list hardware hw_acl
awplus(config-ip-hw-acl)# permit ip any any
awplus(config)# class-map cmap3
awplus(config-cmap)# match access-group hw_acl

Related Commands

class-map
match cos

**Overview** Use this command to define a COS to match against incoming packets. Use the `no` variant of this command to remove CoS.

**Syntax**

- `match cos <0-7>`
- `no match cos`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;0-7&gt;</code></td>
<td>Specify the CoS value.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-63&gt;</td>
<td>Specify DSCP value (only one value can be specified).</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;layer-two-formats&gt;</td>
<td></td>
</tr>
<tr>
<td>802dot2-tagged</td>
<td>802.2 Tagged Packets (enter the parameter name).</td>
</tr>
<tr>
<td>802dot2-untagged</td>
<td>802.2 Untagged Packets (enter the parameter name).</td>
</tr>
<tr>
<td>ethii-tagged</td>
<td>EthII Tagged Packets (enter the parameter name).</td>
</tr>
<tr>
<td>ethii-untagged</td>
<td>EthII Untagged Packets (enter the parameter name).</td>
</tr>
<tr>
<td>ethii-any</td>
<td>EthII Tagged or Untagged Packets (enter the parameter name).</td>
</tr>
<tr>
<td>netwareraw-tagged</td>
<td>Netware Raw Tagged Packets (enter the parameter name).</td>
</tr>
<tr>
<td>netwareraw-untagged</td>
<td>Netware Raw Untagged Packets (enter the parameter name).</td>
</tr>
<tr>
<td>snap-tagged</td>
<td>SNAP Tagged Packets (enter the parameter name).</td>
</tr>
<tr>
<td>snap-untagged</td>
<td>SNAP Untagged Packets (enter the parameter name).</td>
</tr>
<tr>
<td>&lt;layer-three-protocols&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;word&gt;</td>
<td>A Valid Protocol Number in hexidecimal.</td>
</tr>
<tr>
<td>any</td>
<td>Note that the parameter “any” is only valid when used with the netwarerawtagged and netwarerawuntagged protocol options.</td>
</tr>
<tr>
<td>sna-path-control</td>
<td>Protocol Number 04 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>provay-lan</td>
<td>Protocol Number 0E (enter the parameter name or its number).</td>
</tr>
<tr>
<td>eia-rs</td>
<td>Protocol Number 4E (enter the parameter name or its number).</td>
</tr>
<tr>
<td>provay</td>
<td>Protocol Number 8E (enter the parameter name or its number).</td>
</tr>
<tr>
<td>ipx-802dot2</td>
<td>Protocol Number E0 (enter the parameter name or its number).</td>
</tr>
</tbody>
</table>
### QoS COMMANDS

**MATCH ETH-FORMAT PROTOCOL**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>netbeui</td>
<td>Protocol Number F0 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>iso-clns-is</td>
<td>Protocol Number FE (enter the parameter name or its number).</td>
</tr>
<tr>
<td>xdot75-internet</td>
<td>Protocol Number 0801 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>nbs-internet</td>
<td>Protocol Number 0802 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>ecma-internet</td>
<td>Protocol Number 0803 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>chaosnet</td>
<td>Protocol Number 0804 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>xdot25-level-3</td>
<td>Protocol Number 0805 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>arp</td>
<td>Protocol Number 0806 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>xns-compat</td>
<td>Protocol Number 0807 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>banyan-systems</td>
<td>Protocol Number 0BAD (enter the parameter name or its number).</td>
</tr>
<tr>
<td>bbn-simnet</td>
<td>Protocol Number 5208 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>dec-mop-dump-ld</td>
<td>Protocol Number 6001 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>dec-mop-rem-cdons</td>
<td>Protocol Number 6002 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>dec-decnet</td>
<td>Protocol Number 6003 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>dec-lat</td>
<td>Protocol Number 6004 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>dec-diagnostic</td>
<td>Protocol Number 6005 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>dec-customer</td>
<td>Protocol Number 6006 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>dec-lavc</td>
<td>Protocol Number 6007 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>rarp</td>
<td>Protocol Number 8035 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>dec-lanbridge</td>
<td>Protocol Number 8038 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>dec-encryption</td>
<td>Protocol Number 803D (enter the parameter name or its number).</td>
</tr>
</tbody>
</table>
QoS COMMANDS
MATCH ETH-FORMAT PROTOCOL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>appletalk</td>
<td>Protocol Number 809B (enter the parameter name or its number).</td>
</tr>
<tr>
<td>ibm-sna</td>
<td>Protocol Number 80D5 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>appletalk-aarp</td>
<td>Protocol Number 80F3 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>snmp</td>
<td>Protocol Number 814CV.</td>
</tr>
<tr>
<td>ethertalk-2</td>
<td>Protocol Number 809B (enter the parameter name or its number).</td>
</tr>
<tr>
<td>ethertalk-2-aarp</td>
<td>Protocol Number 80F3 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>ipx-snap</td>
<td>Protocol Number 8137 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>ipx-802dot3</td>
<td>Protocol Number FFFF (enter the parameter name or its number).</td>
</tr>
<tr>
<td>ip</td>
<td>Protocol Number 0800 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>ipx</td>
<td>Protocol Number 8137 (enter the parameter name or its number).</td>
</tr>
<tr>
<td>ipv6</td>
<td>Protocol Number 86DD (enter the parameter name or its number).</td>
</tr>
</tbody>
</table>

**Mode**  
Class Map Configuration

**Examples**  
To set the eth-format to ethii-tagged and the protocol to 0800 (IP) for class-map cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match eth-format ethii-tagged protocol 0800
awplus#
awplus(config-cmap)# match eth-format ethii-tagged protocol ip
```

To remove the eth-format and the protocol from the class-map cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match eth-format protocol
```
**match 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
```

**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**

```plaintext
match inner-vlan <1-4094>
no match inner-vlan
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-4094&gt;</code></td>
<td>The VLAN number.</td>
</tr>
</tbody>
</table>

**Mode**  Class Map Configuration

**Usage**  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:

```plaintext
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:

```plaintext
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

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2bcast</td>
<td>Layer 2 Broadcast traffic.</td>
</tr>
<tr>
<td>l2mcast</td>
<td>Layer 2 Multicast traffic.</td>
</tr>
<tr>
<td>l2ucast</td>
<td>Layer 2 Unicast traffic.</td>
</tr>
</tbody>
</table>

**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
```
**QoS COMMANDS**

**MATCH TCP-FLAGS**

**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][rst][syn][urg]}
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ack</td>
<td>Acknowledge.</td>
</tr>
<tr>
<td>fin</td>
<td>Finish.</td>
</tr>
<tr>
<td>psh</td>
<td>Push</td>
</tr>
<tr>
<td>rst</td>
<td>Reset.</td>
</tr>
<tr>
<td>syn</td>
<td>Synchronize.</td>
</tr>
<tr>
<td>urg</td>
<td>Urgent.</td>
</tr>
</tbody>
</table>

**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
```
#### QoS COMMANDS

**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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-7&gt;</td>
<td>The Class of Service, user-priority value.</td>
</tr>
</tbody>
</table>

**Default**
By default, all untagged frames are assigned a CoS value of 0. Note that for tagged frames, the default behavior is not to alter the CoS value.

**Mode**
Interface Configuration

**Example**
To assign a CoS user priority value of 2 to all untagged packets entering ports 1.0.1 to 1.0.6, use the commands:

```bash
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# mls qos cos 2
```
**mls qos enable**

**Overview**  Use this command to globally enable QoS on the switch or stack.

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```
**QoS COMMANDS**

**MLS QOS MAP COS-QUEUE TO**

### mls qos map cos-queue to

**Overview** Use this command to set the default CoS to egress queue mapping. This is the default queue mapping for packets that do not get assigned an egress queue via any other QoS functionality.

Use the **no** variant of this command to reset the cos-queue map back to its default setting. The default mappings for this command are:

<table>
<thead>
<tr>
<th>CoS Priority</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS QUEUE</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>

**Syntax**

- `mls qos map cos-queue <cos-priority> to <queue-number>`
- `no mls qos map cos-queue`

**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`
QoS Commands
MLS Qos Map Premark-DSCP To

mls qos map premark-dscp to

Overview
This command configures the premark-dscp map. It is used when traffic is classified by a class-map that has trust dscp configured. Based on a lookup DSCP, the map determines new QoS settings for the traffic.

The no variant of this command resets the premark-dscp map to its defaults. If no DSCP is specified then all DSCP entries will be reset to their defaults.

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>]

Mode
Global Configuration

Usage
With the trust dscp command set, this command (mls qos map premark-dscp) enables you to make the following changes:

• remap the DSCP (leaving the other settings unchanged)
• remap any or all of CoS, output queue, or bandwidth class values (leaving the DSCP unchanged)

NOTE:
If you attempt to remap both the DSCP and another setting, only the DSCP remap will take effect.

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).
Example To set the entry for DSCP 1 to use a new DSCP of 2, 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-dscp 2 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
```
no police

Overview  Use this command to disable any policer previously configured on the class-map.

Syntax   no police

Mode     Policy Map Class Configuration

Usage    This command disables any policer previously configured on the class-map.

Example  To disable policing on a class-map use the command:

awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# no police
police single-rate action

**Overview**  
Configures a single-rate policer for a class-map.

**Syntax**
```
police
single-rate <cir>
<cbs> <ebs> action {drop-red|remark-transmit}
```

**Mode**  
Policy Map Class Configuration

**Usage**  
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.

<table>
<thead>
<tr>
<th>Color</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>green</td>
<td>The traffic rate is less than the average rate and minimum burst.</td>
</tr>
<tr>
<td>yellow</td>
<td>The traffic rate is between the minimum burst and the maximum burst.</td>
</tr>
<tr>
<td>red</td>
<td>The traffic rate exceeds the average rate and the maximum burst.</td>
</tr>
</tbody>
</table>

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 10 Mbps that drops a sustained burst of traffic over this rate, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# police single-rate 10000 1875000 1875000
action drop-red
```

**Related Commands**

no police  
police twin-rate action  
remark-map
QoS COMMANDS
POLICE TWIN-RATE ACTION

police twin-rate action

**Overview**
Configures a twin-rate policer for a class-map.

**Syntax**
```plaintext
police twin-rate <cir> <pir> <cbs> <pbs> action
{drop-red|remark-transmit}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;cir&gt;</td>
<td>Specify the Committed Information Rate (CIR) (1-40000000 kbps).</td>
</tr>
<tr>
<td>&lt;pir&gt;</td>
<td>Specify the Peak Information Rate (PIR) (1-40000000 kbps).</td>
</tr>
<tr>
<td>&lt;cbs&gt;</td>
<td>Specify the Committed Burst Size (CBS) (0-16777216 bytes).</td>
</tr>
<tr>
<td>&lt;pbs&gt;</td>
<td>Specify the Peak Burst Size (PBS) (0-16777216 bytes).</td>
</tr>
<tr>
<td>action</td>
<td>Specify the action if rate is exceeded.</td>
</tr>
<tr>
<td>drop-red</td>
<td>Drop the red packets.</td>
</tr>
<tr>
<td>remark-transmit</td>
<td>Modify the packets using the remark map, then transmit. You can configure the remark map using the remark-map command.</td>
</tr>
</tbody>
</table>

**Mode**
Policy Map Class Configuration

**Usage**
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, minimum burst size, maximum rate, and maximum burst size.

<table>
<thead>
<tr>
<th>Bandwidth Class</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>green</td>
<td>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.</td>
</tr>
<tr>
<td>yellow</td>
<td>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.</td>
</tr>
<tr>
<td>red</td>
<td>The sum of the number of existing (buffered) bytes plus those arriving at the port per unit time, result in a value that exceeds that set for the PBS.</td>
</tr>
</tbody>
</table>

Using an action of drop-red means that any packets classed as red will be discarded.
QoS COMMANDS
POLICE TWIN-RATE ACTION

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 that uses the premark map to remark any non-conforming traffic, use the commands:

```plaintext
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>
```

**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**
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]`

**Mode**
Interface Configuration.

**Usage**
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}]}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth-class</td>
<td>Specify the bandwidth class of packets to remark.</td>
</tr>
<tr>
<td>green</td>
<td>Remark green packets.</td>
</tr>
<tr>
<td>yellow</td>
<td>Remark yellow packets.</td>
</tr>
<tr>
<td>red</td>
<td>Remark red packets.</td>
</tr>
<tr>
<td>new-dscp</td>
<td>Specify the new DSCP value.</td>
</tr>
<tr>
<td>&lt;0-63&gt;</td>
<td>The DSCP value.</td>
</tr>
<tr>
<td>new-bandwidth-class</td>
<td>Specify the new bandwidth class.</td>
</tr>
<tr>
<td>green</td>
<td>Remark the packet green.</td>
</tr>
<tr>
<td>yellow</td>
<td>Remark the packet yellow.</td>
</tr>
<tr>
<td>red</td>
<td>Remark the packet red.</td>
</tr>
</tbody>
</table>

**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]
o remark new-cos [internal|external|both]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-7&gt;</td>
<td>The new value for the CoS flag and/or the input into the CoS to queue map.</td>
</tr>
<tr>
<td>external</td>
<td>Remarks the CoS flag in the packet.</td>
</tr>
<tr>
<td>internal</td>
<td>Remarks the new-CoS input into the CoS to queue map.</td>
</tr>
<tr>
<td>both</td>
<td>Remarks (with the same value) both the CoS flag in the packet and the input to the CoS to queue map.</td>
</tr>
</tbody>
</table>

**Mode**
Policy Map Class Configuration

**Usage**
The default CoS to Queue mappings are shown in the following table:

<table>
<thead>
<tr>
<th>CoS Value</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress Queue No</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>

The relationship between this command and the CoS to queue map is shown in the following figure.
QoS Commands

REMARK NEW-COS

Figure 34-1: Remarking and the CoS to Q map

The above mapping is set by the command, `mls qos map cos-queue to`, and displayed by the command, `show mls qos maps cos-queue`. With the `remark new-cos` command unset, or set to `external`, the queue mapping takes its input from the Existing CoS Value. With the `remark new-cos` command set to `internal` or `both`, the queue mapping takes its input from the value set by the command, `remark new-cos`. Note that although the CoS to Queue map applies to the whole switch, the `remark new-cos` command applies per individual class-map.

Table 34-1: CoS to egress queue remarking function

<table>
<thead>
<tr>
<th>Input</th>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS field = 1</td>
<td>Remark new-cos (not configured)</td>
<td>CoS value = 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Packet sent to egress queue 0</td>
</tr>
<tr>
<td>CoS field = 1</td>
<td>Remark new-cos 2 external</td>
<td>CoS value = 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Packet sent to egress queue 0</td>
</tr>
<tr>
<td>CoS set to 1</td>
<td>Remark new-cos 2 internal</td>
<td>CoS value = 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Packet sent to egress queue 1</td>
</tr>
<tr>
<td>CoS set to 1</td>
<td>Remark new-cos 2 both</td>
<td>CoS value = 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Packet sent to egress queue 1</td>
</tr>
</tbody>
</table>

Note: This table assumes that the CoS to Queue map is set to its default values.

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 to`

`show mls qos maps cos-queue`
service-policy input

Overview  Use this command to apply a policy-map to the input of an interface.

Use the no variant of this command to remove a policy-map and interface association.

Syntax  service-policy input <policy-map>

no service-policy input <policy-map>

Mode  Interface Configuration

Usage  This command can be applied to switch ports or static channel groups, but not to dynamic (LACP) channel groups.

Example  To apply a policy-map named pmap1 to interface port1.0.2, use the commands:

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# service-policy input pmap1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;policy-map&gt;</td>
<td>Policy map name that will be applied to the input.</td>
</tr>
</tbody>
</table>
set ip next-hop (PBR)

**Overview**
When this command is set, all packets that match a selected class-map will be forwarded to the specified next hop.

The no variant of this command removes the next-hop address (in the context of its policy-map and class-map) from the configuration.

**Syntax**

```
set ip next-hop <ip-addr>
noset ip next-hop
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of the next hop destination.</td>
</tr>
</tbody>
</table>

**Mode**
Policy Map Class Configuration

**Usage**

In typical deployments of policy-based routing, some traffic types require normal routing (i.e. via the routes in the IP routing table) while other traffic types require policy-based routing.

Where the traffic to be policy routed is a subset of the traffic that is to be normally routed, then the configuration is reasonably simple. The policy-map will contain one or more classes that match the traffic to be policy routed, and will have their next-hop configured by this command - `set ip next-hop (PBR)`. The remaining traffic will be conventionally routed according to the rules set for the default class - providing that this is not subject to the `set ip next-hop (PBR)`.

The situation becomes a little more complex where the traffic requiring normal routing is a subset of the traffic to be policy-routed. In this situation the policy-map would need to contain one, or more, classes that match the requirement for normal routing. These classes would not be configured with a `set ip next-hop (PBR)` command. The remaining traffic classes that require normal routing would have the `set ip next-hop (PBR)` command applied to them. Note that this traffic could be just the default class, if ALL other traffic types were to be policy-routed.

Also note that the order in which the classes are configured in the policy-map is important; because traffic is matched against the classes in the order that they were assigned to the policy-map.

For more information, see the “Policy-Based Routing” section of the QoS Feature Overview and Configuration Guide.

**Example**
To forward a packet to a 192.168.1.1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# set ip next-hop 192.168.1.1
```
**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**  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;class-map-name&gt;</code></td>
<td>Name of the class-map.</td>
</tr>
</tbody>
</table>

**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 34-2:  Example output from the show class-map command

```
CLASS-MAP-NAME: cmap1
    Set IP DSCP: 56
    Match IP DSCP: 7
```

**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 34-3: 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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>Switch port.</td>
</tr>
</tbody>
</table>

**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 34-4: Example output from the show mls qos interface command

<table>
<thead>
<tr>
<th>Default CoS: 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Queue: 7</td>
</tr>
<tr>
<td>Number of egress queues: 8</td>
</tr>
<tr>
<td>Queue Set: 1</td>
</tr>
<tr>
<td>Egress Queue: 0</td>
</tr>
<tr>
<td>Status: Enabled</td>
</tr>
<tr>
<td>Scheduler: Strict Priority</td>
</tr>
<tr>
<td>Queue Limit: 12%</td>
</tr>
<tr>
<td>Egress Rate Limit: 0 Kb</td>
</tr>
<tr>
<td>Egress Queue: 1</td>
</tr>
<tr>
<td>Status: Enabled</td>
</tr>
<tr>
<td>Scheduler: Strict Priority</td>
</tr>
<tr>
<td>Queue Limit: 12%</td>
</tr>
<tr>
<td>Egress Rate Limit: 0 Kb</td>
</tr>
<tr>
<td>Egress Queue: 2</td>
</tr>
<tr>
<td>Status: Enabled</td>
</tr>
<tr>
<td>Scheduler: Strict Priority</td>
</tr>
<tr>
<td>Queue Limit: 12%</td>
</tr>
<tr>
<td>Egress Rate Limit: 0 Kb</td>
</tr>
<tr>
<td>Egress Queue: 3</td>
</tr>
<tr>
<td>Status: Enabled</td>
</tr>
<tr>
<td>Scheduler: Wrr Group 2</td>
</tr>
<tr>
<td>Weight: 10</td>
</tr>
<tr>
<td>Queue Limit: 12%</td>
</tr>
<tr>
<td>Egress Rate Limit: 0 Kb</td>
</tr>
<tr>
<td>Egress Queue: 4</td>
</tr>
<tr>
<td>Status: Enabled</td>
</tr>
<tr>
<td>Scheduler: Wrr Group 1</td>
</tr>
<tr>
<td>Weight: 10</td>
</tr>
<tr>
<td>Queue Limit: 12%</td>
</tr>
<tr>
<td>Egress Rate Limit: 0 Kb</td>
</tr>
<tr>
<td>Egress Queue: 5</td>
</tr>
<tr>
<td>Status: Enabled</td>
</tr>
<tr>
<td>Scheduler: Strict Priority</td>
</tr>
<tr>
<td>Queue Limit: 12%</td>
</tr>
<tr>
<td>Egress Rate Limit: 0 Kb</td>
</tr>
<tr>
<td>Egress Queue: 6</td>
</tr>
<tr>
<td>Status: Enabled</td>
</tr>
<tr>
<td>Scheduler: Strict Priority</td>
</tr>
<tr>
<td>Queue Limit: 12%</td>
</tr>
<tr>
<td>Egress Rate Limit: 0 Kb</td>
</tr>
<tr>
<td>Egress Queue: 7</td>
</tr>
<tr>
<td>Status: Enabled</td>
</tr>
<tr>
<td>Scheduler: Strict Priority</td>
</tr>
<tr>
<td>Queue Limit: 12%</td>
</tr>
<tr>
<td>Egress Rate Limit: 0 Kb</td>
</tr>
</tbody>
</table>

Table 34-2: Parameters in the output of the show mls qos interface command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default CoS</td>
<td>The default CoS priority that will be applied to all packets arriving on this interface.</td>
</tr>
<tr>
<td>Default Queue</td>
<td>The default queue that will be applied to all packets arriving on this interface.</td>
</tr>
</tbody>
</table>
### Table 34-2: Parameters in the output of the `show mls qos interface` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of egress queues</td>
<td>The total number of egress queues available on this interface.</td>
</tr>
<tr>
<td>Egress Queue X</td>
<td>Number of this egress queue.</td>
</tr>
<tr>
<td>Status</td>
<td>Queue can either be enabled or disabled.</td>
</tr>
<tr>
<td>Scheduler</td>
<td>The scheduling mode being used for servicing the transmission of packets on this port.</td>
</tr>
<tr>
<td>Queue Limit</td>
<td>The percentage of the port’s buffers that have been allocated to this queue.</td>
</tr>
<tr>
<td>Egress Rate Limit</td>
<td>The amount of traffic that can be transmitted via this queue per second. 0 Kb means there is currently no rate-limiting enabled.</td>
</tr>
</tbody>
</table>
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.

Note that these 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.

**Syntax**
```
show mls qos interface <port> policer-counters [class-map <class-map>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>Switch port.</td>
</tr>
<tr>
<td>class-map</td>
<td>Select a class-map.</td>
</tr>
<tr>
<td>&lt;class-map&gt;</td>
<td>Class-map name.</td>
</tr>
</tbody>
</table>

**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.

**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 34-5: Example output from `show mls qos interface policer-counters`

```
awplus#show mls qos int 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:  1629056
 Red Bytes:           7003200
 Dropped Bytes:       0
 Non-dropped Bytes:   8632256
```
QoS COMMANDS
SHOW MLS QOS INTERFACE POLICER-COUNTERS

This output shows a policer configured with remarking through ‘action remark-transmit’, so although bytes are marked as Red, none are dropped. Therefore, the ‘Non-dropped Bytes’ field shows a summation of Green/Yellow and Red bytes.
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 <0-7>]
```

**Parameter** | **Description**
---|---
<port> | Switch port.
<0-7> | Queue.

**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 34-6: Example output from the `show mls qos interface queue-counters` command

```
Interface port1.0.4 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 34-3: Parameters in the output of the `show mls qos interface queue-counters` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Port we are showing the counters for.</td>
</tr>
<tr>
<td>Port queue length</td>
<td>Number of frames in the port’s queue. This will be the sum of all egress queues on the port.</td>
</tr>
<tr>
<td>Egress Queue length</td>
<td>Number of frames in a specific egress queue.</td>
</tr>
</tbody>
</table>
**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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port&gt;</td>
<td>Switch port.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Example**  
To see the QSP status on port1.0.1, use command:  
```
awplus# show mls qos interface port1.0.1 storm-status
```

**Output**  
Figure 34-7: Example output from the `show mls qos interface storm-status` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface:</td>
<td>port1.0.1</td>
</tr>
<tr>
<td>Storm-Protection:</td>
<td>Enabled</td>
</tr>
<tr>
<td>Port-status:</td>
<td>Enabled</td>
</tr>
<tr>
<td>Storm Action:</td>
<td>vlandisable</td>
</tr>
<tr>
<td>Storm Window:</td>
<td>5000 ms</td>
</tr>
<tr>
<td>Storm Downtime:</td>
<td>0 s</td>
</tr>
<tr>
<td>Timeout Remaining:</td>
<td>0 s</td>
</tr>
<tr>
<td>Last read data-rate:</td>
<td>0 kbps</td>
</tr>
<tr>
<td>Storm Rate:</td>
<td>1000 kbps</td>
</tr>
</tbody>
</table>

**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 34-8:  Example output from the show mls qos maps cos-queue command

<table>
<thead>
<tr>
<th>COS-TO-QUEUE-MAP:</th>
<th>0 1 2 3 4 5 6 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>COS :</td>
<td>0 2 3 4 5 6 7</td>
</tr>
<tr>
<td>QUEUE:</td>
<td>0 1 3 4 5 6 7</td>
</tr>
</tbody>
</table>

Related Commands  mls qos map cos-queue to
### show mls qos maps premark-dscp

**Overview**  This command displays the premark-dscp map. This map is used when the `trust dscp` command has been specified for a policy-map’s class-map 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>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-63&gt;</td>
<td>DSCP table entry.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**  To display the premark-dscp map for DSCP 1, use the command:

```bash
awplus# show mls qos maps premark-dscp 1
```

**Output**  Figure 34-9: 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 to trust dscp`
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>]`

**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 34-10: Example output from the show policy-map command

```
POLICY-MAP-NAME: general-traffic
   State: attached
       Default class-map action: permit
   CLASS-MAP-NAME: default
   CLASS-MAP-NAME: database-traffic
```

**Related Commands**  
`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.
- **linkdown** will physically bring the port down. The **vlandisable** requires the match vlan class-map to be present in the class-map.

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
```

**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
```

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-86400&gt;</td>
<td>Seconds.</td>
</tr>
</tbody>
</table>
**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**
- `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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-40000000&gt;</code></td>
<td>The range of the storm-rate.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;100-60000&gt;</td>
<td>The window size, measured in milliseconds.</td>
</tr>
</tbody>
</table>

**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 bandwidth-class, CoS, DSCP, and queue 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. Because policy-maps are applied to ports, you can think of **trust dscp** as a per-port setting.

**Examples**

To enable the premark-dscp map lookup for policy-map pmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# trust dscp
```

To disable the premark-dscp map lookup for policy-map pmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# no trust
```

**Related Commands**  
mls qos map premark-dscp to
**wrr-queue 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]

**Mode**
Interface Configuration

**Examples**
To disable queue 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 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 651Kb.

**Syntax**  
```
wrr-queue egress-rate-limit <bandwidth> queues {0}[1][2][3][4][5][6][7]
```
```
o wrr-queue egress-rate-limit <bandwidth>
queues {0}[1][2][3][4][5][6][7]
```

**Mode**  Interface Configuration

**Example**  To limit the egress rate of queues 0, 1 and 2, 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;bandwidth&gt;</td>
<td>Bandwidth &lt;1-40000000 kbits&gt; (usable units: k, m, g).</td>
</tr>
<tr>
<td>{0}[1]...[7]</td>
<td>Selects one or more queues to apply the bandwidth limit to as specified in the preceding &lt;bandwidth&gt; parameter.</td>
</tr>
</tbody>
</table>
wrr-queue weight queues

**Overview**
This command configures weighted round-robin based scheduling on the specified egress queues on switch port interfaces only. The weights are specified as ratios relative to each other.

**Syntax**
```
wrr-queue weight <1-15> queues [0][1][2][3][4][5][6][7]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-15&gt;</td>
<td>Weight (the higher the number the greater will be the queue servicing).</td>
</tr>
<tr>
<td>[0][1]...[7]</td>
<td>Enter egress queue numbers 0-7, to assign the specified queues the specified weight.</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration for switch port interfaces only (not for static aggregated interfaces).

**Usage**
Only apply weighted round-robin based scheduling to switch port interfaces (for example, `awplus(config)#interface port1.0.2`).

You cannot apply weighted round-robin based scheduling to static aggregated interfaces (for example, `awplus(config)#interface sa2`). Attempting to apply weighted round-robin based scheduling on aggregated interfaces will display the console error shown below:
```
awplus# configure terminal
awplus(config)# interface sa2
awplus(config-if)# wrr-queue weight
% Invalid input detected at ^ marker
```

**Example**
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
```

**Related Commands**
- priority-queue
- show mls qos interface
802.1X Commands

Introduction

Overview
This chapter provides an alphabetical reference of commands used to configure 802.1X port access control.

Command List

- “debug dot1x” on page 1483
- “dot1x control-direction” on page 1484
- “dot1x eap” on page 1485
- “dot1x eapol-version” on page 1486
- “dot1x initialize interface” on page 1487
- “dot1x initialize supplicant” on page 1488
- “dot1x keytransmit” on page 1489
- “dot1x max-auth-fail” on page 1490
- “dot1x max-reauth-req” on page 1492
- “dot1x port-control” on page 1493
- “dot1x timeout tx-period” on page 1495
- “show debugging dot1x” on page 1496
- “show dot1x” on page 1497
- “show dot1x diagnostics” on page 1500
- “show dot1x interface” on page 1502
- “show dot1x sessionstatistics” on page 1507
- “show dot1x statistics interface” on page 1508
- “show dot1x supplicant” on page 1509
- “show dot1x supplicant interface” on page 1511
- “undebug dot1x” on page 1514
**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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Used with the <strong>no</strong> variant of this command exclusively; turns off all debugging for 802.1X.</td>
</tr>
<tr>
<td>auth-web</td>
<td>Specifies debugging for 802.1X auth-web information.</td>
</tr>
<tr>
<td>events</td>
<td>Specifies debugging for 802.1X events.</td>
</tr>
<tr>
<td>nsm</td>
<td>Specifies debugging for NSM messages.</td>
</tr>
<tr>
<td>packet</td>
<td>Specifies debugging for 802.1X packets.</td>
</tr>
<tr>
<td>timer</td>
<td>Specifies debugging for 802.1X timers.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec and Global Configuration

**Usage**  
This command without any parameters turns on normal 802.1X debug information.

```
awplus# debug dot1x
awplus# show debugging dot1x
```

802.1X debugging status:

- 802.1X events debugging is on
- 802.1X timer debugging is on
- 802.1X packets debugging is on
- 802.1X NSM debugging is on

**Examples**  
awplus# debug dot1x
awplus# debug dot1x all

**Related Commands**  
show debugging dot1x
undebug dot1x
**dot1x control-direction**

**Overview**  
This command sets the direction of the filter for the unauthorized interface.  
If the optional **in** parameter is specified with this command then packets entering the specified port are discarded. The **in** parameter discards the ingress packets received from the supplicant.  
If the optional **both** parameter is specified with this command then packets entering (ingress) and leaving (egress) the specified port are discarded. The **both** parameter discards the packets received from the supplicant and sent to the supplicant.  
The **no** variant of this command sets the direction of the filter to **both**. The port will then discard both ingress and egress traffic.

**Syntax**  
dot1x control-direction {in|both}  
no dot1x control-direction

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>Discard received packets from the supplicant (ingress packets).</td>
</tr>
<tr>
<td>both</td>
<td>Discard received packets from the supplicant (ingress packets) and transmitted packets to the supplicant (egress packets).</td>
</tr>
</tbody>
</table>

**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.

**Examples**  
To set the port direction to the default (**both**) for port1.0.2, use the commands:  
```plaintext  
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:  
```plaintext  
awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# dot1x control-direction in  
```

**Validation Commands**
- show dot1x  
- show dot1x interface  
- show auth-mac interface  
- show auth-web interface
**dot1x eap**

**Overview**  
This command selects the transmit mode for the EAP packet. If the authentication feature is not enabled then EAP transmit mode is not enabled. The default setting discards EAP packets.

**Syntax**  
dot1x eap {discard|forward|forward-untagged-vlan|forward-vlan}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>discard</td>
<td>Discard.</td>
</tr>
<tr>
<td>forward</td>
<td>Forward to all ports on the switch.</td>
</tr>
<tr>
<td>forward-untagged-vlan</td>
<td>Forward to ports with the same untagged VLAN.</td>
</tr>
<tr>
<td>forward-vlan</td>
<td>Forward to ports with the same VLAN.</td>
</tr>
</tbody>
</table>

**Default**  
The transmit mode is set to `discard` EAP packets by default.

**Mode**  
Global Configuration

**Examples**  
To set the transmit mode of EAP packet to `forward` to forward EAP packets to all ports on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward
```

To set the transmit mode of EAP packet to `discard` to discard EAP packets, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap discard
```

To set the transmit mode of EAP packet to `forward-untagged-vlan` to forward EAP packets to ports with the same untagged vlan, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward-untagged-vlan
```

To set the transmit mode of EAP packet to `forward-vlan` to forward EAP packets to ports with the same vlan, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward-vlan
```
dot1x eapol-version

Overview  This command sets the EAPOL protocol version for EAP packets when 802.1X port authentication is applied.

Use the no variant of this command to set the EAPOL protocol version to 1.

The default EAPOL protocol version is version 1.

Syntax  dot1x eapol-version {1|2}
no dot1x eapol-version

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EAPOL version.</td>
</tr>
<tr>
<td>2</td>
<td>EAPOL version.</td>
</tr>
</tbody>
</table>

Default  The EAP version for 802.1X authentication is set to 1 by default.

Mode  Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples  To set the EAPOL protocol version to 2 for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x eapol-version 2
```

To set the EAPOL protocol version to the default version (1) for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x eapol-version
```

Validation Commands  show dot1x
show dot1x interface
dot1x initialize interface

**Overview**
This command removes authorization for a connected interface with the specified <interface-list>. The connection will attempt to re-authorize when the specified port attempts to make use of the network connection.

*NOTE:* Reauthentication could be a long time after the use of this command because the reauthorization attempt is not triggered by this command. The attempt is triggered by the first packet from the interface trying to access the network resources.

**Syntax**
dot1x initialize interface <interface-list>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-list&gt;</td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• 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)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. vlan2-8, or port1.0.1-1.0.6, or sa1-2, or po1-2</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above; e.g. port1.0.1, port1.0.2-1.0.4. Do not mix interface types in a list</td>
</tr>
<tr>
<td></td>
<td>The specified interfaces must exist.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Examples**
To initialize 802.1X port authentication on the interface port1.0.2, use the command:

```markdown
awplus# dot1x initialize interface port1.0.2
```

To unauthorize switch port1.0.1 and attempt reauthentication on switch port1.0.1, use the command:

```markdown
awplus# dot1x initialize interface port1.0.1
```

To unauthorize all switch ports for a 24-port device and attempt reauthentication, use the command:

```markdown
awplus# dot1x initialize interface port1.0.1-port1.0.24
```

**Validation Commands**
show dot1x
show dot1x interface

**Related Commands**
dot1x initialize supplicant
dot1x initialize supplicant

**Overview**  This command removes authorization for a connected supplicant with the specified MAC address or username. The connection will attempt to re-authorize when the specified supplicant attempts to make use of the network connection.

*NOTE:* Reauthentication could be a long time after the use of this command because the reauthorization attempt is not triggered by this command. The attempt is triggered by the first packet from the supplicant trying to access the network resources.

**Syntax**  
dot1x initialize supplicant {<macadd>|username}

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x</td>
<td>IEEE 802.1X Port-Based Access Control.</td>
</tr>
<tr>
<td>initialize</td>
<td>Initialize the port to attempt reauthentication.</td>
</tr>
<tr>
<td>supplicant</td>
<td>Specify the supplicant to initialize.</td>
</tr>
<tr>
<td>&lt;macadd&gt;</td>
<td>MAC (hardware address of the supplicant.</td>
</tr>
<tr>
<td>username</td>
<td>The name of the supplicant entry.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Example**  To initialize the supplicant authentication, use the commands

```
awplus# configure terminal
awplus(config)# dot1x initialize supplicant 0090.99ab.a020
awplus(config)# dot1x initialize supplicant guest
```

**Validation Commands**

- show dot1x
- show dot1x supplicant

**Related Commands**

- dot1x initialize interface
dot1x keytransmit

**Overview**  This command enables key transmission on the interface specified previously in Interface mode.

The `no` variant of this command disables key transmission on the interface specified.

**Syntax**

```
dot1x keytransmit
no dot1x keytransmit
```

**Default**  Key transmission for port authentication is enabled by default.

**Mode**  Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**  Use this command to enable key transmission over an Extensible Authentication Protocol (EAP) packet between the authenticator and supplicant. Use the `no` variant of this command to disable key transmission.

**Examples**  To enable the key transmit feature on interface `port1.0.2`, after it has been disabled by negation, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x keytransmit
```

To disable the key transmit feature from the default startup configuration on interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x keytransmit
```

**Validation Commands**

- `show dot1x`
- `show dot1x interface`
dot1x max-auth-fail

**Overview**  Use this command to configure the maximum number of login attempts for a supplicant (client device) using the **auth-fail vlan** feature, when using 802.1X port authentication on an interface.

The **no** variant of this command resets the maximum login attempts for a supplicant (client device) using the auth-fail vlan feature, to the default configuration of 3 login attempts.

**Syntax**  
```
dot1x max-auth-fail <0-10>
no dot1x max-auth-fail
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-10&gt;</td>
<td>Specify the maximum number of login attempts for supplicants on an interface using 802.1X port authentication.</td>
</tr>
</tbody>
</table>

**Default**  The default maximum number of login attempts for a supplicant on an interface using 802.1X port authentication is three (3) login attempts.

**Mode**  Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**  This command sets the maximum number of login attempts for supplicants on an interface. The supplicant is moved to the auth-fail VLAN from the Guest VLAN after the number of failed login attempts using 802.1X authentication is equal to the number set with this command.

See the **Authentication Feature Overview and Configuration Guide** for information about:

- the auth-fail VLAN feature, and
- restrictions regarding combinations of authentication enhancements working together

**Examples**  To configure the maximum number of login attempts for a supplicant on interface port1.0.2 to a single (1) login attempt, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x max-auth-fail 1
```

To configure the maximum number of login attempts for a supplicant on interface port1.0.2 to the default number of three (3) login attempts, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x max-auth-fail
```
802.1X COMMANDS
DOT1X MAX-AUTH-FAIL

**Validation Commands**
show running-config

**Related Commands**
auth auth-fail vlan
dot1x max-reauth-req
show dot1x interface
dot1x max-reauth-req

**Overview**  This command sets the number of reauthentication attempts before an interface is unauthorized.

The no variant of this command resets the reauthentication delay to the default.

**Syntax**
```
dot1x max-reauth-req <1-10>
no dot1x max-reauth-req
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-10&gt;</td>
<td>Specify the maximum number of reauthentication attempts for supplicants on an interface using 802.1X port authentication.</td>
</tr>
</tbody>
</table>

**Default**  The default maximum reauthentication attempts for interfaces using 802.1X port authentication is two (2) reauthentication attempts, before an interface is unauthorized.

**Mode**  Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**  Use this command to set the maximum reauthentication attempts after failure.

**Examples**
To configure the maximum number of reauthentication attempts for interface port1.0.2 to a single (1) reauthentication request, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x max-reauth-req 1
```

To configure the maximum number of reauthentication attempts for interface port1.0.2 to the default maximum number of two (2) reauthentication attempts, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x max-reauth-req
```

**Validation Commands**
show running-config

**Related Commands**
dot1x max-auth-fail
show dot1x interface
dot1x port-control

**Overview**
This command enables 802.1X port authentication on the interface specified, and sets the control of the authentication port. When `port-control` is set to `auto`, the 802.1X authentication feature is executed on the interface, but only if the `aaa authentication dot1x` command has been issued.

The `no` variant of this command disables the port authentication on the interface specified.

**Syntax**
```
dot1x port-control {force-unauthorized|force-authorized|auto}
no dot1x port-control
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>force-unauthorized</td>
<td>Force port state to unauthorized. Specify to force a port to always be in an unauthorized state.</td>
</tr>
<tr>
<td>force-authorized</td>
<td>Force port state to authorized. Specify to force a port to always be in an authorized state.</td>
</tr>
<tr>
<td>auto</td>
<td>Allow port client to negotiate authentication. Specify to enable authentication on port.</td>
</tr>
</tbody>
</table>

**Default**
802.1X port control is disabled by default.

**Mode**
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**
Use this command to force a port state. Note that all `dot1x` commands can only be applied to switch ports. They cannot be applied to dynamic (LACP) or static channel groups.

**Examples**
To enable port authentication on the interface `port1.0.2`, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
```

To enable port authentication force authorized on the interface `port1.0.2`, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control force-authorized
```
To disable port authentication on the interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x port-control
```

**Validation Commands**

- `show dot1x interface`

**Related Commands**

- `aaa authentication dot1x`
dot1x timeout tx-period

**Overview**  This command sets the transmit timeout for the authentication request on the specified interface.

The `no` variant of this command resets the transmit timeout period to the default (30 seconds).

**Syntax**  
```
dot1x timeout tx-period <1-65535>
nodot1x timeout tx-period
```

**Default**  The default transmit period for port authentication is 30 seconds.

**Mode**  Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**  Use this command to set the interval between successive attempts to request an ID.

**Examples**  To set the transmit timeout period to 5 seconds on interface `port1.0.2`, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x timeout tx-period 5
```

To reset transmit timeout period to the default (30 seconds) on interface `port1.0.2`, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# nodot1x timeout tx-period
```

**Validation Commands**  
- `show dot1x`
- `show dot1x interface`
**show debugging dot1x**

**Overview**  Use this command to display the 802.1X debugging option set.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
```
show debugging dot1x
```

**Mode**  User Exec and Privileged Exec

**Usage**  
This is a sample output from the `show debugging dot1x` command.

```
awplus# debug dot1x
awplus# show debugging dot1x

802.1X debugging status:
  802.1X events debugging is on
  802.1X timer debugging is on
  802.1X packets debugging is on
  802.1X NSM debugging is on
```

**Example**  
```
awplus# show debugging dot1x
```

**Related Commands**  
`debug dot1x`
show dot1x

Overview
This command shows authentication information for dot1x (802.1X) port authentication.

If you specify the optional all parameter then this command also displays all authentication information for each port available on the switch.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Syntax
show dot1x [all]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all authentication information for each port available on the switch.</td>
</tr>
</tbody>
</table>

Mode
Privileged Exec

Example
awplus# show dot1x all
Table 35-1: Example output from the `show dot1x` command

```
awplus# show dot1x all
802.1X Port-Based Authentication Enabled
RADIUS server address: 150.87.18.89:1812
Next radius message id: 5
RADIUS client address: not configured
Authentication info for interface port1.0.6
portEnabled: true - portControl: Auto
portStatus: Authorized
reAuthenticate: disabled
reAuthPeriod: 3600
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
PAE: connectTimeout: 30
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in
KT: keyTxEnabled: false
critical: disabled
guestVlan: disabled
dynamicVlanCreation: single-dynamic-vlan
assignFailActionRule: deny
hostMode: multi-suppliant
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
```
### Table 35-1: Example output from the `show dot1x` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>supplicantMac</td>
<td>none</td>
</tr>
<tr>
<td>Supplicant name</td>
<td>manager</td>
</tr>
<tr>
<td>Supplicant address</td>
<td>00d0.59ab.7037</td>
</tr>
<tr>
<td>authenticationMethod</td>
<td>802.1X Authentication</td>
</tr>
<tr>
<td>portStatus</td>
<td>Authorized - currentId: 1</td>
</tr>
<tr>
<td>abort</td>
<td>F</td>
</tr>
<tr>
<td>start</td>
<td>F</td>
</tr>
<tr>
<td>timeout</td>
<td>F</td>
</tr>
<tr>
<td>success</td>
<td>T</td>
</tr>
<tr>
<td>PAE quietPeriod</td>
<td>60</td>
</tr>
<tr>
<td>maxReauthReq</td>
<td>2</td>
</tr>
<tr>
<td>txPeriod</td>
<td>30</td>
</tr>
<tr>
<td>BE state</td>
<td>Idle</td>
</tr>
<tr>
<td>reqCount</td>
<td>0</td>
</tr>
<tr>
<td>idFromServer</td>
<td>0</td>
</tr>
<tr>
<td>CD bridgeDetected</td>
<td>false</td>
</tr>
<tr>
<td>criticalState</td>
<td>off</td>
</tr>
<tr>
<td>dynamicVlanId</td>
<td>2</td>
</tr>
<tr>
<td>802.1X statistics for interface port1.0.6</td>
<td></td>
</tr>
<tr>
<td>EAPOL Frames Rx</td>
<td>5</td>
</tr>
<tr>
<td>EAPOL Frames Tx</td>
<td>16</td>
</tr>
<tr>
<td>EAPOL Start Frames Rx</td>
<td>0</td>
</tr>
<tr>
<td>EAPOL Logoff Frames Rx</td>
<td>0</td>
</tr>
<tr>
<td>EAP Rsp/Id Frames Rx</td>
<td>3</td>
</tr>
<tr>
<td>EAP Response Frames Rx</td>
<td>2</td>
</tr>
<tr>
<td>EAP Req/Id Frames Tx</td>
<td>8</td>
</tr>
<tr>
<td>EAP Request Frames Tx</td>
<td>2</td>
</tr>
<tr>
<td>Invalid EAPOL Frames Rx</td>
<td>0</td>
</tr>
<tr>
<td>EAPOL Last Frame Version Rx</td>
<td>1</td>
</tr>
<tr>
<td>EAPOL Last Frame Src</td>
<td>00d0.59ab.7037</td>
</tr>
<tr>
<td>Authentication session statistics for interface port1.0.6</td>
<td></td>
</tr>
<tr>
<td>session user name</td>
<td>manager</td>
</tr>
<tr>
<td>session authentication method</td>
<td>Remote server</td>
</tr>
<tr>
<td>session time</td>
<td>19440 secs</td>
</tr>
<tr>
<td>session terminate cause</td>
<td>Not terminated yet</td>
</tr>
</tbody>
</table>

### Authentication Diagnostics for interface port1.0.6

<table>
<thead>
<tr>
<th>Event</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>authEnterConnecting</td>
<td>2</td>
</tr>
<tr>
<td>authEaplogoffWhileConnecting</td>
<td>1</td>
</tr>
<tr>
<td>authEnterAuthenticating</td>
<td>2</td>
</tr>
<tr>
<td>authSuccessWhileAuthenticating</td>
<td>1</td>
</tr>
<tr>
<td>authTimeoutWhileAuthenticating</td>
<td>1</td>
</tr>
<tr>
<td>authFailWhileAuthenticating</td>
<td>0</td>
</tr>
<tr>
<td>authEapstartWhileAuthenticating</td>
<td>0</td>
</tr>
<tr>
<td>authEaplogoffWhileAuthenticating</td>
<td>0</td>
</tr>
<tr>
<td>authReauthsWhileAuthenticated</td>
<td>0</td>
</tr>
<tr>
<td>authEapstartWhileAuthenticated</td>
<td>0</td>
</tr>
<tr>
<td>authEaplogoffWhileAuthenticated</td>
<td>0</td>
</tr>
<tr>
<td>BackendResponses</td>
<td>2</td>
</tr>
<tr>
<td>BackendAccessChallenges</td>
<td>1</td>
</tr>
<tr>
<td>BackendOtherrequestToSupplicant</td>
<td>3</td>
</tr>
<tr>
<td>BackendAuthSuccess</td>
<td>1</td>
</tr>
<tr>
<td>BackendAuthFails</td>
<td>0</td>
</tr>
</tbody>
</table>
show dot1x diagnostics

**Overview**
This command shows 802.1X authentication diagnostics for the specified interface (optional), which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
show dot1x diagnostics [interface <interface-list>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specify a port to show.</td>
</tr>
<tr>
<td>&lt;interface-list&gt;</td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>- 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)</td>
</tr>
<tr>
<td></td>
<td>- 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</td>
</tr>
<tr>
<td></td>
<td>- a comma-separated list of the above; e.g. port1.0.1, port1.0.2-1.0.4. Do not mix interface types in a list</td>
</tr>
<tr>
<td></td>
<td>The specified interfaces must exist.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
See the sample output below showing 802.1X authentication diagnostics for port1.0.5:

awplus# show dot1x diagnostics interface port1.0.5
Output

Figure 35-1: Example output from the show dot1x diagnostics command

```
Authentication Diagnostics for interface port1.0.5
    Supplicant address: 00d0.59ab.7037
    authEnterConnecting: 2
    authEaplogoffWhileConnecting: 1
    authEnterAuthenticating: 2
    authSuccessWhileAuthenticating: 1
    authTimeoutWhileAuthenticating: 1
    authFailWhileAuthenticating: 0
    authEapstartWhileAuthenticating: 0
    authEaplogoffWhileAuthenticating: 0
    authReauthsWhileAuthenticated: 0
    authEapstartWhileAuthenticated: 0
    authEaplogoffWhileAuthenticated: 0
    BackendResponses: 2
    BackendAccessChallenges: 1
    BackendOtherrequestToSupplicant: 3
    BackendAuthSuccess: 1
```
show dot1x interface

**Overview**
This command shows the status of 802.1X port-based authentication on the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interfaces. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interfaces. Use the optional **statistics** parameter to show authentication diagnostics for the specified interfaces. Use the optional **supplicant** parameter to show the supplicant state for the specified interfaces.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show dot1x interface <interface-list>
[diagnostics|sessionstatistics|statistics|supplicant [brief]]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-list&gt;</td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• 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)</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above; e.g. port1.0.1, port1.0.3-1.0.5. Do not mix interface types in a list</td>
</tr>
<tr>
<td></td>
<td>The specified interfaces must exist.</td>
</tr>
<tr>
<td>diagnostics</td>
<td>Diagnostics.</td>
</tr>
<tr>
<td>sessionstatistics</td>
<td>Session Statistics.</td>
</tr>
<tr>
<td>statistics</td>
<td>Statistics.</td>
</tr>
<tr>
<td>supplicant</td>
<td>Supplicant.</td>
</tr>
<tr>
<td>brief</td>
<td>Brief summary of supplicant state.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Examples**
See the sample output below showing 802.1X authentication status for port1.0.6:

```
awplus# show dot1x interface port1.0.6
```
802.1X COMMANDS

SHOW DOT1X INTERFACE

Table 35-2: Example output from the `show dot1x interface` command for a port

```
awplus# show dot1x interface port1.0.6
Authentication info for interface port1.0.6
portEnabled: true - portControl: Auto
portStatus: Authorized
reAuthenticate: disabled
reAuthPeriod: 3600
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
PAE: connectTimeout: 30
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in
KT: keyTxEnabled: false
critical: disabled
guestVlan: disabled
dynamicVlanCreation: single-dynamic-vlan
assignFailActionRule: deny
hostMode: multi-suppliant
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
```

See the sample output below showing 802.1X authentication session statistics for port1.0.6:

```
awplus# show dot1x interface port1.0.6 sessionstatistics
```

```
awplus# show dot1x interface port1.0.6
sessionstatistics
Authentication session statistics for interface port1.0.6
session user name: manager
    session authentication method: Remote server
    session time: 19440 secs
    session terminat cause: Not terminated yet
```

See sample output below showing 802.1X authentication diagnostics for port1.0.6:

```
awplus# show dot1x interface port1.0.6 diagnostics
```
802.1X COMMANDS
SHOW DOT1X INTERFACE

See sample output below showing the supplicant on the interface port1.0.6:

```
awplus# show dot1x interface port1.0.6 supplicant

authenticationMethod: dot1x
portStatus: Authorized - currentId: 4
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 -
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing 802.1X (dot1x) authentication statistics for port1.0.6:

```
awplus# show dot1x statistics interface port1.0.6
```

See sample output below showing the supplicant on the interface port1.0.6:

```
awplus# show dot1x interface port1.0.6 supplicant

authenticationMethod: dot1x
portStatus: Authorized - currentId: 4
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 -
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
```
### 802.1X COMMANDS

#### SHOW DOT1X INTERFACE

```
awplus#show dot1x statistics interface port1.0.6
802.1X statistics
for interface port1.0.6
  EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
  EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
  EAP Resp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
  EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
  EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame
    Src:00d0.59ab.7037
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portEnabled</td>
<td>Interface operational status (Up-true/down-false).</td>
</tr>
<tr>
<td>portControl</td>
<td>Current control status of the port for 802.1X control.</td>
</tr>
<tr>
<td>portStatus</td>
<td>802.1X status of the port (authorized/unauthorized).</td>
</tr>
<tr>
<td>reAuthenticate</td>
<td>Reauthentication enabled/disabled status on port.</td>
</tr>
<tr>
<td>reAuthPeriod</td>
<td>Value holds meaning only if reauthentication is enabled.</td>
</tr>
<tr>
<td>abort</td>
<td>Indicates that authentication should be aborted when set to true.</td>
</tr>
<tr>
<td>fail</td>
<td>Indicates failed authentication attempt when set to false.</td>
</tr>
<tr>
<td>start</td>
<td>Indicates authentication should be started when set to true.</td>
</tr>
<tr>
<td>timeout</td>
<td>Indicates authentication attempt timed out when set to true.</td>
</tr>
<tr>
<td>success</td>
<td>Indicates authentication successful when set to true.</td>
</tr>
<tr>
<td>state</td>
<td>Current 802.1X operational state of interface.</td>
</tr>
<tr>
<td>mode</td>
<td>Configured 802.1X mode.</td>
</tr>
<tr>
<td>reAuthCount</td>
<td>Reauthentication count.</td>
</tr>
<tr>
<td>quietperiod</td>
<td>Time between reauthentication attempts.</td>
</tr>
<tr>
<td>reAuthMax</td>
<td>Maximum reauthentication attempts.</td>
</tr>
<tr>
<td>BE</td>
<td>Backend authentication state machine variables and constants.</td>
</tr>
<tr>
<td>state</td>
<td>State of the state machine.</td>
</tr>
<tr>
<td>reqCount</td>
<td>Count of requests sent to server.</td>
</tr>
<tr>
<td>suppTimeout</td>
<td>Supplicant timeout.</td>
</tr>
</tbody>
</table>
Table 35-3: Parameters in the output of `show dot1x interface` (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>serverTimeout</td>
<td>Server timeout.</td>
</tr>
<tr>
<td>maxReq</td>
<td>Maximum requests to be sent.</td>
</tr>
<tr>
<td>CD</td>
<td>Controlled Directions State machine.</td>
</tr>
<tr>
<td>adminControlledDirections</td>
<td>Administrative value (Both/In).</td>
</tr>
<tr>
<td>operControlledDirections</td>
<td>Operational Value (Both/In).</td>
</tr>
<tr>
<td>KR</td>
<td>Key receive state machine.</td>
</tr>
<tr>
<td>rxKey</td>
<td>True when EAPOL-Key message is received by supplicant or authenticator.</td>
</tr>
<tr>
<td>KT</td>
<td>Key Transmit State machine.</td>
</tr>
<tr>
<td>keyAvailable</td>
<td>False when key has been transmitted by authenticator, true when new key is</td>
</tr>
<tr>
<td></td>
<td>available for key exchange.</td>
</tr>
<tr>
<td>keyTxEnabled</td>
<td>Key transmission enabled/disabled status.</td>
</tr>
</tbody>
</table>

**Related Commands**
- `show auth-web diagnostics`
- `show dot1x sessionstatistics`
- `show dot1x statistics interface`
- `show dot1x supplicant interface`
show dot1x sessionstatistics

**Overview**
This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show dot1x sessionstatistics [interface <interface-list>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specify a port to show.</td>
</tr>
</tbody>
</table>
| <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**
See sample output below showing 802.1X (dot1x) authentication session statistics for port1.0.6:
```
awplus# show dot1x sessionstatistics interface port1.0.6
```

```
Authentication session statistics for interface port1.0.6
  session user name: manager
  session authentication method: Remote server
  session time: 19440 secs
  session terminat cause: Not terminated yet
```
show dot1x statistics interface

**Overview**
This command shows the authentication statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show dot1x statistics interface <interface-list>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface-list&gt;</code></td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• an interface (e.g. vlan2), a switch port (e.g. port1.0.6),</td>
</tr>
<tr>
<td></td>
<td>a static channel group (e.g. sa2) or a dynamic (LACP)</td>
</tr>
<tr>
<td></td>
<td>channel group (e.g. po2)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of interfaces, ports, static channel</td>
</tr>
<tr>
<td></td>
<td>groups or dynamic (LACP) channel groups separated by a</td>
</tr>
<tr>
<td></td>
<td>hyphen; e.g. vlan2-8, or port1.0.1-1.0.4, or sa1-2,</td>
</tr>
<tr>
<td></td>
<td>or po1-2</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above; e.g.</td>
</tr>
<tr>
<td></td>
<td>port1.0.1, port1.0.4-1.0.6. Do not mix interface types</td>
</tr>
<tr>
<td></td>
<td>in a list</td>
</tr>
<tr>
<td></td>
<td>The specified interfaces must exist.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
See sample output below showing 802.1X authentication statistics for port1.0.6:
```
awplus# show dot1x statistics interface port1.0.6
```

```
802.1X statistics for interface port1.0.6
  EAPOL Frames Rx:  5 - EAPOL Frames Tx: 16
  EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
  EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
  EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
  EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame
  Src:00d0.59ab.7037
```
show dot1x supplicant

**Overview**
This command shows the supplicant state of the authentication mode set for the switch.

This command shows a summary when the optional **brief** parameter is used.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show dot1x supplicant [<macadd>] [brief]
```

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;macadd&gt;</code></td>
<td>MAC (hardware) address of the Supplicant.</td>
</tr>
<tr>
<td><strong>brief</strong></td>
<td>Brief summary of the Supplicant state.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
See sample output below showing the 802.1X authenticated supplicant on the switch:

```
awplus# show dot1x supplicant

authenticationMethod: dot1x
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
PAE: state: Authenticated - portMode: Auto
PAE: reAuthCount: 0 - rxRespId: 0
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 3
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
```
See sample output below showing the supplicant on the switch using the `brief` parameter:

```
awplus# show dot1x supplicant 00d0.59ab.7037 brief
```

```
Interface port1.0.6
  authenticationMethod: dot1x/web
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
    webBasedAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address    Status            IP Address      Username
------------- ----- ----- =========== ============= =========== =============== =======
port1.0.6     5   W    0008.0d5e.c216 Authenticated     192.168.1.200   web
```

For example, if two-step authentication is configured with 802.1X authentication as the first method and web authentication as the second method then the output is as follows:

```
Interface port1.0.6 authenticationMethod: dot1x/web
Two-Step Authentication
  firstMethod: dot1x
  secondMethod: web
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 0
    webBasedAuthenticationSupplicantNum: 1
    otherAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address    Status            IP Address      Username
------------- ----- ----- =========== ============= =========== =============== =======
port1.0.6     5   W    0008.0d5e.c216 Authenticated     192.168.1.200   web
```

**Related Commands**

- `show dot1x supplicant interface`
show dot1x supplicant interface

**Overview**
This command shows the supplicant state of the authentication mode set for the interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

This command shows a summary when the optional `brief` parameter is used.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show dot1x supplicant interface <interface-list> [brief]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface-list&gt;</code></td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• 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)</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>The specified interfaces must exist.</td>
</tr>
</tbody>
</table>

**brief**
Brief summary of the Supplicant state.

**Mode**
Privileged Exec

**Examples**
See sample output below showing the supplicant on the interface `port1.0.6`:
```
awplus# show dot1x interface port1.0.6
```
802.1X COMMANDS
SHOW DOT1X SUPPLICANT INTERFACE

See sample output below showing the supplicant on the switch using the `brief` parameter:

```
awplus# show dot1x supplicant interface brief
```

```
Interface port1.0.6
  authenticationMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
  macBasedAuthenticationSupplicantNum: 0
  dot1xAuthenticationSupplicantNum: 1
  webBasedAuthenticationSupplicantNum: 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
    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

  Interface port1.0.6 authenticationMethod: dot1x
    totalSupplicantNum: 1
    authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    webBasedAuthenticationSupplicantNum: 0

  Interface   VID  Mode MAC Address     Status          IP Address      Username
  =========   ===  ==== ===========     ======          ==========      ========
  port1.0.6   2    D  00d0.59ab.7037  Authenticated   192.168.2.201   manager
```

See the sample output below for static channel group (static aggregator) interface `sa1`:

```
awplus# show dot1x interface sa1 supplicant brief
```

```
See sample output below showing the supplicant on the switch using the `brief` parameter:

```
awplus# show dot1x supplicant interface brief
```

```
Interface port1.0.6
  authenticationMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
  macBasedAuthenticationSupplicantNum: 0
  dot1xAuthenticationSupplicantNum: 1
  webBasedAuthenticationSupplicantNum: 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
    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

  Interface port1.0.6 authenticationMethod: dot1x
    totalSupplicantNum: 1
    authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    webBasedAuthenticationSupplicantNum: 0

  Interface   VID  Mode MAC Address     Status          IP Address      Username
  =========   ===  ==== ===========     ======          ==========      ========
  port1.0.6   2    D  00d0.59ab.7037  Authenticated   192.168.2.201   manager
```

See the sample output below for static channel group (static aggregator) interface `sa1`:
SHOW DOT1X SUPPLICANT INTERFACE

```
awplus#show dot1x interface sa1 supplicant brief
Interface sa1
  authenticationMethod: dot1x
Two-Step Authentication:
  firstMethod: mac
  secondMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    webBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>VID</th>
<th>Mode</th>
<th>MAC Address</th>
<th>Status</th>
<th>IP Address</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>sa1</td>
<td>1</td>
<td>D</td>
<td>00d0.59ab.7037</td>
<td>Authenticated</td>
<td>--</td>
<td>test1</td>
</tr>
</tbody>
</table>
```

Related Commands
show dot1x supplicant
**Overview**  This command applies the functionality of the **no** variant of the `debug dot1x` command.
Introduction

**Overview**  This chapter provides an alphabetical reference for authentication commands.
AUTHENTICATION COMMANDS

**Command List**

- “auth auth-fail vlan” on page 1520
- “auth critical” on page 1522
- “auth dynamic-vlan-creation” on page 1523
- “auth guest-vlan” on page 1526
- “auth host-mode” on page 1528
- “auth log” on page 1530
- “auth max-supplicant” on page 1532
- “auth reauthentication” on page 1533
- “auth roaming disconnected” on page 1534
- “auth roaming enable” on page 1536
- “auth supplicant-mac” on page 1538
- “auth timeout connect-timeout” on page 1540
- “auth timeout quiet-period” on page 1541
- “auth timeout reauth-period” on page 1542
- “auth timeout server-timeout” on page 1543
- “auth timeout supp-timeout” on page 1544
- “auth two-step enable” on page 1545
- “auth-mac enable” on page 1548
- “auth-mac method” on page 1550
- “auth-mac password” on page 1551
- “auth-mac reauth-relearning” on page 1552
- “auth-web enable” on page 1553
- “auth-web forward” on page 1554
- “auth-web max-auth-fail” on page 1556
- “auth-web method” on page 1557
- “auth-web-server blocking-mode” on page 1558
- “auth-web-server dhcp ipaddress” on page 1559
- “auth-web-server dhcp lease” on page 1560
- “auth-web-server dhcp-wpad-option” on page 1561
- “auth-web-server gateway (deleted)” on page 1562
- “auth-web-server host-name” on page 1563
- “auth-web-server http-redirect (deleted)” on page 1564
- “auth-web-server intercept-port” on page 1565
- “auth-web-server ipaddress” on page 1566
- “auth-web-server login-url” on page 1567
AUTHENTICATION COMMANDS

- “auth-web-server mode (deleted)” on page 1568
- “auth-web-server page logo” on page 1569
- “auth-web-server page sub-title” on page 1570
- “auth-web-server page success-message” on page 1571
- “auth-web-server page title” on page 1572
- “auth-web-server page welcome-message” on page 1573
- “auth-web-server ping-poll enable” on page 1574
- “auth-web-server ping-poll failcount” on page 1575
- “auth-web-server ping-poll interval” on page 1576
- “auth-web-server ping-poll reauth-timer-refresh” on page 1577
- “auth-web-server ping-poll timeout” on page 1578
- “auth-web-server port” on page 1579
- “auth-web-server redirect-delay-time” on page 1580
- “auth-web-server redirect-url” on page 1581
- “auth-web-server session-keep” on page 1582
- “auth-web-server ssl” on page 1583
- “auth-web-server sslport (deleted)” on page 1584
- “auth-web-server ssl intercept-port” on page 1585
- “copy proxy-autoconfig-file” on page 1586
- “copy web-auth-https-file” on page 1587
- “erase proxy-autoconfig-file” on page 1588
- “erase web-auth-https-file” on page 1589
- “platform l3-vlan-hashing-algorithm” on page 1590
- “platform mac-vlan-hashing-algorithm” on page 1591
- “show auth two-step supplicant brief” on page 1592
- “show auth-mac” on page 1593
- “show auth-mac diagnostics” on page 1594
- “show auth-mac interface” on page 1595
- “show auth-mac sessionstatistics” on page 1597
- “show auth-mac statistics interface” on page 1598
- “show auth-mac supplicant” on page 1599
- “show auth-mac supplicant interface” on page 1601
- “show auth-web” on page 1602
- “show auth-web diagnostics” on page 1604
- “show auth-web interface” on page 1606
AUTHENTICATION COMMANDS

- “show auth-web sessionstatistics” on page 1609
- “show auth-web statistics interface” on page 1610
- “show auth-web supplicant” on page 1611
- “show auth-web supplicant interface” on page 1612
- “show auth-web-server” on page 1613
- “show auth-web-server page” on page 1614
- “show proxy-autoconfig-file” on page 1615
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4094&gt;</td>
<td>Assigns the VLAN ID to any supplicants that have failed port authentication.</td>
</tr>
</tbody>
</table>

**Default**  
The **auth-fail vlan** feature is disabled by default.

**Mode**  
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**  
Use the **auth-fail vlan** feature when using Web-Authentication instead of the Guest VLAN feature, when you need to separate networks where one supplicant (client device) requires authentication and another supplicant does not require authentication from the same interface.

This is because the DHCP lease time using the Web-Authentication feature is shorter, and the **auth fail vlan** feature enables assignment to a different VLAN if a supplicant fails authentication.

To enable the **auth-fail vlan** feature with Web Authentication, you need to set Web Authentication Server virtual IP address by using the **auth-web-server ipaddress** command or the **auth-web-server dhcp ipaddress** command.

When using 802.1X port authentication, use a **dot1x max-auth-fail** command to set the maximum number of login attempts. Three login attempts are allowed by default for 802.1X port authentication before supplicants trying to authenticate are moved from the Guest VLAN to the auth-fail VLAN. See the **dot1x max-auth-fail** on page 1490 for command information.

See the Authentication Feature Overview and Configuration Guide for information about:

- the auth-fail VLAN feature, which allows the Network Administrator to separate the supplicants who attempted authentication, but failed, from the supplicants who did not attempt authentication, and
- restrictions regarding combinations of authentication enhancements working together

Use appropriate ACLs (Access Control Lists) on interfaces for extra security if a supplicant allocated to the designated auth-fail vlan can access the same network.
AUTH AUTH-FAIL VLAN

as a supplicant on the Guest VLAN. For more information about ACL concepts, and configuring ACLs see the ACL Feature Overview and Configuration Guide. For more information about ACL commands see:

**Examples**

To enable auth-fail vlan for port1.0.2 and assign VLAN 100, use the following commands:

```bash
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:

```bash
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth auth-fail vlan
```

**Validation Commands**

show running-config

**Related Commands**

dot1x max-auth-fail
show dot1x
show dot1x interface
**auth critical**

**Overview**
This command enables the critical port feature on the interface. When the critical port feature is enabled on an interface, and all the RADIUS servers are unavailable, then the interface becomes authorized.

The **no** variant of this command disables critical port feature on the interface.

**Syntax**
- `auth critical`
- `no auth critical`

**Default**
The critical port of port authentication is disabled.

**Mode**
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples**
To enable the critical port feature on interface `port1.0.2`, use the following commands:

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

To disable the critical port feature on interface `port1.0.2`, use the following commands:

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

**Validation Commands**
- `show auth-web-server`
- `show dot1x`
- `show dot1x interface`
- `show running-config`
AUTHENTICATION COMMANDS

AUTH DYNAMIC-VLAN-CREATION

auth dynamic-vlan-creation

**Overview**
This command enables and disables the Dynamic VLAN assignment feature.

The Dynamic VLAN assignment feature allows a supplicant (client device) to be placed into a specific VLAN based on information returned from the RADIUS server during authentication, on a given interface.

Use the **no** variant of this command to disable the Dynamic VLAN assignment feature.

**Syntax**
auth dynamic-vlan-creation [rule {deny|permit}] [type {multi|single}]
no auth dynamic-vlan-creation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule</td>
<td>VLAN assignment rule.</td>
</tr>
<tr>
<td>deny</td>
<td>Deny a differently assigned VLAN ID. This is the default rule.</td>
</tr>
<tr>
<td>permit</td>
<td>Permit a differently assigned VLAN ID.</td>
</tr>
<tr>
<td>type</td>
<td>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.</td>
</tr>
<tr>
<td>multi</td>
<td>Multiple Dynamic VLAN.</td>
</tr>
<tr>
<td>single</td>
<td>Single Dynamic VLAN.</td>
</tr>
</tbody>
</table>

**Default**
By default, the Dynamic VLAN assignment feature is disabled.

**Mode**
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**
If the Dynamic VLAN assignment feature is enabled (disabled by default), VLAN assignment is dynamic. If the Dynamic VLAN assignment feature is disabled then RADIUS attributes are ignored and configured VLANs are assigned to ports. Dynamic VLANs may be associated with authenticated MAC addresses if the **type** parameter is applied with the **rule** parameter.

The **rule** parameter deals with the case where there are multiple supplicants attached to a port, and the type parameter has been set to **single-vlan**. The parameter specifies how the switch should act if different VLAN IDs end up being assigned to different supplicants. The keyword value **deny** means that once a given VID has been assigned to the first supplicant, then if any subsequent supplicant is assigned a different VID, that supplicant is rejected. The keyword value **permit** means that once a given VID has been assigned to the first supplicant, then if any subsequent supplicant is assigned a different VID, that supplicant is accepted, but it is actually assigned the same VID as the first supplicant.
AUTHENTICATION COMMANDS

AUTH DYNAMIC-VLAN-CREATION

If you issue an auth dynamic-vlan-creation command without an optional rule parameter and a required deny or permit keyword value then a second supplicant with a different VLAN ID is rejected. It is not assigned to the first supplicant’s VLAN. Issuing an auth dynamic-vlan-creation command without an optional rule parameter has the same effect as issuing an auth dynamic-vlan-creation rule deny command rejecting supplicants with differing 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-suppliant. For single-host ports, the VLAN ID will be assigned to the port. It is not supported with the Guest VLAN feature. Display the ID assigned using a show vlan command. For multi-host ports, the VLAN ID will be assigned to the MAC address of the authenticated supplicant. The VLAN ID assigned for the MAC Base VLAN is displayed using the show platform table vlan command.

To configure Dynamic Vlan with Web Authentication, you need to set Web Authentication Server virtual IP address by using the auth-web-server ipaddress command or the auth-web-server dhcp ipaddress command. You also need to create a hardware access-list that can be applied to the switch port interface.

You need to configure an IPv4 address for the VLAN interface on which Web Authentication is running.

**Examples**

To enable the Dynamic VLAN assignment feature on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport access vlan 10
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# interface vlan10
awplus(config-if)# ip address 10.1.1.1/24
```

To enable the Dynamic VLAN assignment feature with Web Authentication on interface port1.0.2 when Web Authentication is needed, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ipaddress 1.2.3.4
awplus(config)# access-list hardware acl-web send-to-cpu ip any 1.2.3.4
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# access-group acl-web
awplus(config-if)# interface vlan1
awplus(config-if)# ip address 10.1.1.1/24
```
To disable the Dynamic VLAN assignment feature on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth dynamic-vlan-creation
```

Validation Commands
- `show dot1x`
- `show dot1x interface`
- `show running-config`

Related Commands
- `auth host-mode`
**auth guest-vlan**

**Overview**  
This command enables and configures the Guest VLAN feature on the interface specified by associating a Guest VLAN with an interface. This command does not start authentication. The supplicant's (client device's) traffic is associated with the native VLAN of the interface if it's not already associated with another VLAN. The `routing` option enables routing from the Guest VLAN to another VLAN, so the switch can lease DHCP addresses and accept access to a limited network.

The no variant of this command disables the guest vlan feature on the interface specified.

**Syntax**  
auth guest-vlan <1-4094> [routing]

no auth guest-vlan [routing]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4094&gt;</td>
<td>VLAN ID (VID).</td>
</tr>
<tr>
<td>routing</td>
<td>Enables routing from the Guest VLAN to other VLANs.</td>
</tr>
</tbody>
</table>

**Default**  
The Guest VLAN authentication feature is disabled by default.

**Mode**  
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**  
The Guest VLAN feature may be used by supplicants (client devices) that have not attempted authentication, or have failed the authentication process. Note that if a port is in multi-suppliant mode with per-port dynamic VLAN configuration, after the first successful authentication, subsequent hosts cannot use the guest VLAN due to the change in VLAN ID. This may be avoided by using per-user dynamic VLAN assignment.

When using the Guest VLAN feature with the multi-host mode, a number of supplicants can communicate via a guest VLAN before authentication. A supplicant's traffic is associated with the native VLAN of the specified switch port. The supplicant must belong to a VLAN before traffic from the supplicant can be associated.

Note that you must first define the VLAN with the `vlan` command that you will assign as a guest VLAN using this command. Also note that 802.1X must first be enabled on the port.

Guest VLAN authentication cannot be enabled if DHCP snooping is enabled (service dhcp-snooping command), and vice versa.

The Guest VLAN feature in previous releases had some limitations that have been removed. Until this release the Guest VLAN feature could not lease the IP address to the supplicant using DHCP Server or DHCP Relay features unless Web-Authentication was also applied. When using NAP authentication, the supplicant should have been able to log on to a domain controller to gain certification, but the Guest VLAN would not accept access to another VLAN.
The Guest VLAN routing mode in this release overcomes these issues. With the Guest VLAN routing mode, the switch can lease DHCP addresses and accept access to a limited network.

Note that Guest VLAN can use only untagged ports and tagged ports cannot be used for Guest VLAN.

See the Authentication Feature Overview and Configuration Guide for information about:

- Guest VLAN, and
- restrictions regarding combinations of authentication enhancements working together

**Examples**

To define vlan100 and assign the guest VLAN feature to vlan100 on interface port1.0.2, and enable routing from the guest vlan to other VLANs, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 100
awplus(config-vlan)# exit
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth guest-vlan 100 routing
```

To disable the guest vlan feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth guest-vlan
```

**Validation Commands**

- show dot1x
- show dot1x interface
- show running-config

**Related Commands**

- dot1x port-control
- vlan
**auth host-mode**

**Overview**  This command selects host mode on the interface. Multi-host is an extension to IEEE802.1X.

*Use the no variant of this command to set host mode to the default setting (single host).*

**Syntax**  
```
auth host-mode {single-host|multi-host|multi-suppliant}
no auth host-mode
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>single-host</td>
<td>Single host mode. In this mode, only one host may be authorized with the port. If other hosts out the interface attempt to authenticate, the authenticator blocks the attempt.</td>
</tr>
<tr>
<td>multi-host</td>
<td>Multi host mode. In this mode, multiple hosts may be authorized with the port; however only one host must be successfully authenticated at the Authentication Server for all hosts to be authorized with the port. Upon one host being successfully authenticated (state Authenticated), the other hosts will be automatically authorized at the port (state ForceAuthorized). If no host is successfully authenticated, then all hosts are not authorized with the port.</td>
</tr>
<tr>
<td>multi-suppliant</td>
<td>Multi supplicant (client device) mode. In this mode, multiple hosts may be authorized with the port, but each host must be individually authenticated with the Authentication Server to be authorized with the port. Supplicants which are not authenticated are not authorized with the port, while supplicants which are successfully authenticated are authorized with the port.</td>
</tr>
</tbody>
</table>

**Default**  The default host mode for port authentication is for a single host.

**Mode**  Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**  Ports residing in the unauthorized state for host(s) or supplicant(s), change to an authorized state when the host or supplicant has successfully authenticated with the Authentication Server.

When multi-host mode is used or auth critical feature is used, all hosts do not need to be authenticated.
**Examples**

To set the host mode to multi-suppliant 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-suppliant
```

To set the host mode to default (single host) on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth host-mode
```

**Validation Commands**

- `show dot1x`
- `show dot1x interface`
- `show running-config`
AUTHENTICATION COMMANDS

AUTH LOG

auth log

Overview
Use this command to configure the types of authentication feature log messages that are output to the log file.

Use the no variant of this command to remove either specified types or all types of authentication feature log messages that are output to the log file.

Syntax

```
auth log {dot1x|auth-mac|auth-web} {success|failure|logoff|all}
no auth log {dot1x|auth-mac|auth-web} {success|failure|logoff|all}
```

Parameter | Description
--- | ---
dot1x | Specify only 802.1X-Authentication log messages are output to the log file.
auth-mac | Specify only MAC-Authentication log messages are output to the log file.
auth-web | Specify only Web-Authentication log messages are output to the log file.
success | Specify only successful authentication log messages are output to the log file.
failure | Specify only authentication failure log messages are output to the log file.
logoff | Specify only authentication log-off messages are output to the log file. Note that link down, age out and expired ping polling messages will be included.
all | Specify all types of authentication log messages are output to the log file. Note that this is the default behavior for the authentication logging feature.

Default
All types of authentication log messages are output to the log file by default.

Mode
Interface Configuration

Examples
To configure the logging of MAC-Authentication failures to the log file for supplicants (client devices) connected to interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth log auth-mac failure
```
To configure the logging of all types of authentication log messages to the log file for supplicants (client devices) connected to interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth log all
```

**Validation Commands**

`show running-config`
**auth max-suppliant**

**Overview**
This command sets the maximum number of supplicants (client devices) on the interface that can be authenticated. After this value is exceeded supplicants are not authenticated.

The **no** variant of this command resets the maximum supplicant number to the default (1024).

**Syntax**
```
auth max-suppliant <2-1024>
no auth max-suppliant
```

**Default**
The max supplicant of port authentication is 1024.

**Mode**
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples**
To set the maximum number of supplicants to 10 on interface port1.0.2, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth max-suppliant 10
```

To reset the maximum number of supplicant to default on interface port1.0.2, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth max-suppliant
```

**Validation Commands**
- `show dot1x`
- `show dot1x interface`
- `show running-config`
**auth reauthentication**

**Overview**
This command enables re-authentication on the interface specified in the Interface mode, which may be a static channel group (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the `no` variant of this command to 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.

**Examples**
To enable reauthentication on interface `port1.0.2`, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth reauthentication
```

**Validation Commands**
- `show dot1x`
- `show dot1x interface`
- `show running-config`
auth roaming disconnected

**Overview**
This command enables the Roaming Authentication feature on an authenticated interface that is link down. A supplicant (a client device) is not reauthenticated when moved between authenticated interfaces, providing both interfaces have the Roaming Authentication feature enabled before the supplicant is moved.

Use the `auth roaming enable` command before using this command. The `auth roaming disconnected` command on its own will have no effect on the operation of the switch. This command will only come into effect once the base Roaming Authentication feature is enabled, using the `auth roaming enable` command.

The `no` variant of this command disables the Roaming Authentication feature on an interface, and forces a supplicant to be reauthenticated when moving between interfaces.

See the Authentication Feature Overview and Configuration Guide for further information about this feature.

**Syntax**

```plaintext
auth roaming disconnected

no auth roaming disconnected
```

**Default**
The Roaming Authentication disconnected feature is disabled by default on an interface. Authentication status for a roaming supplicant is deleted by default when an interface goes down.

**Mode**
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**
This command allows a supplicant to move to another authenticating interface without reauthentication, if the link is down for the interface that the supplicant is moved from.

Note that 802.1X port authentication, or MAC-Authentication, or Web-Authentication must first be enabled on an interface to use this feature. The port that the supplicant is moving to must have the same authentication configuration as the port the supplicant is moving from.

Configure `auth roaming enable` on an interface before configuring `auth roaming disconnected` if you require `auth roaming disconnected` configured on an interface for a roaming supplicant.

Roaming Authentication cannot be enabled if DHCP snooping is enabled (service dhcp-snooping command), and vice versa.
**Examples**

To enable Roaming Authentication disconnected feature for port1.0.2, after enabling 802.1X-Authentication and enabling Roaming Authentication enable, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth roaming enable
awplus(config-if)# auth roaming disconnected
```

To disable Roaming Authentication disconnected feature for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth roaming disconnected
```

**Validation Commands**

show running-config

**Related Commands**

auth-mac enable
auth roaming enable
auth-web enable
dot1x port-control
show auth-mac interface
show auth-web interface
show dot1x interface
auth roaming enable

**Overview**  This command enables the Roaming Authentication feature on an authenticated interface that is link up. A supplicant (a client device) is not reauthenticated when moved between authenticated interfaces, providing both interfaces have the Roaming Authentication feature enabled before the supplicant is moved.

Use the `auth roaming enable` command before using `auth roaming disconnected` command. The `auth roaming disconnected` command on its own will have no effect on the operation of the switch. This command will only come into effect once the base Roaming Authentication feature is enabled, using the `auth roaming enable` command.

The `no` variant of this command disables the Roaming Authentication feature on an interface, and forces a supplicant to be reauthenticated when moving between interfaces.

See the Authentication Feature Overview and Configuration Guide for further information about this feature.

**Syntax**  
```
auth roaming enable
no auth roaming enable
```

**Default**  
The Roaming Authentication enable feature is disabled by default on an interface.

Authentication status for a roaming supplicant is deleted by default when an interface goes down.

**Mode**  
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**  
This command allows a supplicant to move to another authenticating interface without reauthentication, providing the link is up for the interface that the supplicant is moved from.

Note that 802.1X port authentication, or MAC-Authentication, or Web-Authentication must first be enabled on an interface to use this feature. The port that the supplicant is moving to must have the same authentication configuration as the port the supplicant is moving from.

Configure `auth roaming enable` on an interface before configuring `auth roaming disconnected` if you require `auth roaming disconnected` configured on an interface for a roaming supplicant.

Roaming Authentication cannot be enabled if DHCP snooping is enabled (service dhcp-snooping command), and vice versa.
AUTHENTICATION COMMANDS

AUTH ROAMING ENABLE

**Examples**

To enable the Roaming Authentication enable feature for interface `port1.0.4`, after enabling 802.1X-Authentication, since an authentication method is required, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth roaming enable
```

To disable Roaming Authentication enable for `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no auth roaming enable
```

**Validation Commands**

`show running-config`

**Related Commands**

- `auth-mac enable`
- `auth roaming disconnected`
- `auth-web enable`
- `dot1x port-control`
- `show auth-mac interface`
- `show auth-web interface`
- `show dot1x interface`
auth supplicant-mac

**Overview**
This command adds a supplicant (client device) MAC address on a given interface with the parameters as specified in the table below.

Use the `no` variant of this command to delete the supplicant MAC address added by the `auth supplicant-mac` command, and resets to the default for the supplicant parameter.

**Syntax**
```
auth supplicant <mac-addr> [max-reauth-req <1-10>]
   [port-control
   {auto|force-authorized|force-unauthorized|skip-second-auth}]
   [quiet-period <1-65535>]
   [reauth-period <1-4294967295>]
   [supp-timeout <1-65535>]
   [server-timeout <1-65535>]
   [reauthentication]
```
```
o auth supplicant-mac <macadd> [reauthentication]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mac-addr&gt;</code></td>
<td>MAC (hardware) address of the Supplicant entry in HHHH.HHHH.HHHH MAC address hexadecimal format.</td>
</tr>
<tr>
<td>port-control</td>
<td>Port control commands.</td>
</tr>
<tr>
<td>auto</td>
<td>Allow port client to negotiate authentication.</td>
</tr>
<tr>
<td>force-authorized</td>
<td>Force port state to authorized.</td>
</tr>
<tr>
<td>force-unauthorized</td>
<td>Force port state to unauthorized.</td>
</tr>
<tr>
<td>skip-second-auth</td>
<td>Skip the second authentication.</td>
</tr>
<tr>
<td>quiet-period</td>
<td>Quiet period in the HELD state (default 60 seconds).</td>
</tr>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>Seconds for quiet period.</td>
</tr>
<tr>
<td>reauth-period</td>
<td>Seconds between reauthorization attempts (default 3600 seconds).</td>
</tr>
<tr>
<td><code>&lt;1-4294967295&gt;</code></td>
<td>Seconds for reauthorization attempts (reauth-period).</td>
</tr>
<tr>
<td>supp-timeout</td>
<td>Supplicant response timeout (default 30 seconds).</td>
</tr>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>Seconds for supplicant response timeout.</td>
</tr>
<tr>
<td>server-timeout</td>
<td>Authentication server response timeout (default 30 seconds).</td>
</tr>
<tr>
<td><code>&lt;1-65535&gt;</code></td>
<td>Seconds for authentication server response timeout.</td>
</tr>
<tr>
<td>reauthentication</td>
<td>Enable reauthentication on a port.</td>
</tr>
<tr>
<td>max-reauth-req</td>
<td>No of reauthentication attempts before becoming unauthorized (default 2).</td>
</tr>
<tr>
<td><code>&lt;1-10&gt;</code></td>
<td>Count of reauthentication attempts.</td>
</tr>
</tbody>
</table>
AUTHENTICATION COMMANDS

AUTH SUPPLICANT-MAC

Default

No supplicant MAC address for port authentication exists by default until first created with the `auth supplicant-mac` command. The defaults for parameters applied are as shown in the table.

Mode

Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples

To add the supplicant MAC address 0009.41A4.5943 to force authorized port control for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth supplicant-mac 0009.41A4.5943 port-control force-authorized
```

To delete the supplicant MAC address 0009.41A4.5943 for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth supplicant-mac 0009.41A4.5943
```

To reset reauthentication to disable for the supplicant MAC address 0009.41A4.5943, for interface port1.0.2 use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth supplicant-mac 0009.41A4.5943 reauthentication
```

Validation Commands

show dot1x
show dot1x interface
show running-config
AUTHENTICATION COMMANDS
AUTH TIMEOUT CONNECT-TIMEOUT

auth timeout connect-timeout

**Overview**
This command sets the connect-timeout period for the interface.
Use the **no** variant of this command to reset the connect-timeout period to the default (30 seconds).

**Syntax**
- auth timeout connect-timeout &lt;1-65535&gt;
- no auth timeout connect-timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Seconds.</td>
</tr>
</tbody>
</table>

**Default**
The connect-timeout default is 30 seconds.

**Mode**
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**
This command is used for MAC- and Web-Authentication. If the connect-timeout has lapsed and the supplicant has the state **connecting**, then the supplicant is deleted. When **auth-web-server session-keep** or **auth two-step enable** is enabled, we recommend you configure a longer connect-timeout period.

**Examples**
To set the connect-timeout period to 3600 for interface port1.0.2, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout connect-timeout 3600
```
To reset the connect-timeout period to the default (30 seconds) for interface port1.0.2, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout connect-timeout
```

**Validation Commands**
- show dot1x
- show dot1x interface
auth timeout quiet-period

**Overview**
This command sets the time period for which the authentication request is not accepted on a given interface, after the authentication request has failed an authentication.

Use the no variant of this command to reset quiet period to the default (60 seconds).

**Syntax**

```
auth timeout quiet-period <1-65535>
no auth timeout quiet-period
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Seconds.</td>
</tr>
</tbody>
</table>

**Default**
The quiet period of port authentication is 60 seconds.

**Mode**
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples**
To set the quiet period to 10 for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout quiet-period 10
```

To reset the quiet period to the default (60 seconds) for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout quiet-period
```
**auth timeout reauth-period**

**Overview**  
This command sets the timer for reauthentication on a given interface. The re-authentication for the supplicant (client device) is executed at this timeout. The timeout is only applied if the **auth reauthentication** command is applied.

Use the `no` variant of this command to reset the `reauth-period` parameter to the default (3600 seconds).

**Syntax**
```
auth timeout reauth-period <1-4294967295>
no auth timeout reauth-period
```

**Default**  
The default reauthentication period for port authentication is 3600 seconds, when reauthentication is enabled on the port.

**Mode**  
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples**  
To set the reauthentication period to 1 day for interface `port1.0.2`, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout reauth-period 86400
```
To reset the reauthentication period to the default (3600 seconds) for interface `port1.0.2`, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout reauth-period
```

**Validation Commands**
- `show dot1x`
- `show dot1x interface`
- `show running-config`

**Related Commands**
- `auth reauthentication`
auth timeout server-timeout

**Overview**
This command sets the timeout for the waiting response from the RADIUS server on a given interface.

The **no** variant of this command resets the server-timeout to the default (30 seconds).

**Syntax**
auth timeout server-timeout <1-65535>
no auth timeout server-timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Seconds.</td>
</tr>
</tbody>
</table>

**Default**
The server timeout for port authentication is 30 seconds.

**Mode**
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples**
To set the server timeout to 120 seconds for interface **port1.0.2**, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout server-timeout 120
```

To set the server timeout to the default (30 seconds) for interface **port1.0.2**, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout server-timeout
```

**Validation Commands**
- `show dot1x`
- `show dot1x interface`
- `show running-config`
auth timeout supp-timeout

Overview
This command sets the timeout of the waiting response from the supplicant (client device) on a given interface.

The no variant of this command resets the supplicant timeout to the default (30 seconds).

Syntax
auth timeout supp-timeout <1-65535>
no auth timeout supp-timeout

Default
The supplicant timeout of port authentication is 30 seconds.

Mode
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Examples
To set the server timeout to 2 seconds for interface port1.0.2, use the following commands:

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout supp-timeout 2

To reset the server timeout to the default (30 seconds) for interface port1.0.2, use the following commands:

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout supp-timeout

Validation
Commands
show dot1x
show dot1x interface
show running-config
auth two-step enable

**Overview**  This command enables a two-step authentication feature on an interface. When this feature is enabled, the supplicant is authorized in a two-step process. If authentication succeeds, the supplicant becomes authenticated. This command will apply the two-step authentication method based on 802.1X-, MAC- or Web-Authentication.

The **no** variant of this command disables the two-step authentication feature.

**Syntax**  
auth two-step enable
no auth two-step enable

**Default**  Default.

**Mode**  Interface Configuration for a port.

**Usage**  The single step authentication methods (either user or device authentication) have a potential security risk:

- an unauthorized user can access the network with an authorized device, or
- an authorized user can access the network with an unauthorized device.

Two-step authentication solves this problem by authenticating both the user and the device. The supplicant will only become authenticated if both these steps are successful. If the first authentication step fails, then the second step is not started.

**Examples**  To enable the two step authentication feature, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth two-step enable
```

To disable the two step authentication feature, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth two-step enable
```
AUTHENTICATION COMMANDS

AUTH TWO-STEP ENABLE

To enable MAC-Authentication followed by 802.1X-Authentication, use the following commands:

```bash
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:

```bash
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:

```bash
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-web enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

**Validation Commands**

- `show startup-config`
- `show auth-mac supplicant`
- `show dot1x supplicant`
AUTHENTICATION COMMANDS

AUTH TWO-STEP ENABLE

Related Commands

show auth two-step supplicant brief
show auth-mac
show auth-mac interface
show auth-mac supplicant
show auth-web
show auth-web interface
show auth-web supplicant
show dot1x
show dot1x interface
show dot1x supplicant
**auth-mac enable**

**Overview**  
This command enables MAC-based authentication on the interface specified in the Interface command mode.  

Use the no variant of this command to disable MAC-based authentication on an interface.

**Syntax**  
auth-mac enable  
no auth-mac enable

**Default**  
MAC-Authentication is disabled by default.

**Mode**  
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**  
Enabling `spanning-tree edgeport` on ports after enabling MAC-based authentication avoids unnecessary re-authentication when the port state changes, which does not happen when spanning tree edgeport is enabled. Note that re-authentication is correct behavior without `spanning-tree edgeport` enabled.

Applying `switchport mode access` on ports is also good practice to set the ports to access mode with ingress filtering turned on, whenever ports for MAC-Authentication are in a VLAN.

**Examples**  
To enable MAC-Authentication on interface `port1.0.2` and enable spanning tree edgeport to avoid unnecessary re-authentication, use the following commands:

```
awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# auth-mac enable  
awplus(config-if)# spanning-tree edgeport  
awplus(config-if)# switchport mode access
```

To disable MAC-Authentication on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# no auth-mac enable
```

**Validation Commands**  
show auth-mac  
show auth-mac interface  
show running-config
AUTHENTICATION COMMANDS

**AUTH-MAC ENABLE**

**Related Commands**

- aaa accounting auth-mac default
- aaa authentication auth-mac
- spanning-tree edgeport (RSTP and MSTP)
- switchport mode access
AUTHENTICATION COMMANDS

AUTH-MAC METHOD

**auth-mac method**

**Overview**
This command sets the type of authentication method for MAC-Authentication that is used with RADIUS on the interface specified in the Interface command mode.

The `no` variant of this command resets the authentication method used to the default method (PAP) as the RADIUS authentication method used by the MAC-Authentication.

**Syntax**

```
auth-mac method [eap-md5|pap]
no auth-mac method
```

**Parameter** | **Description**
--- | ---
eap-md5 | Enable EAP-MD5 of authentication method.
pap | Enable PAP of authentication method.

**Default**
The MAC-Authentication method is PAP.

**Mode**
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples**
To set the MAC-Authentication method to **pap** on interface **port1.0.2**, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac method pap
```

To set the MAC-Authentication method to the default on interface **port1.0.2**, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-mac method
```

**Validation Commands**

- `show auth-mac`
- `show auth-mac interface`
- `show running-config`
auth-mac password

**Overview**  This command changes the password for MAC-based authentication. Use the *no* variant of this command to return the password to its default.

**Syntax**  
```
auth-mac [encrypted] password <password>
no auth-mac password
```

**Parameter** | **Description**
--- | ---
auth-mac | MAC-based authentication
encrypted | Specify an encrypted password
password | Configure the password
<password> | The new password. Passwords can be up to 64 characters in length and can contain any printable characters except:
  * ?
  * " (double quotes)
  * space

**Default**  By default, the password is the MAC address of the supplicant

**Mode**  Global Configuration

**Usage**  Changing the password increases the security of MAC-based authentication, because the default password is easy for an attacker to discover. This is particularly important if:

  - some MAC-based supplicants on the network are intelligent devices, such as computers, and/or
  - you are using two-step authentication (see the “Ensuring Authentication Methods Require Different Usernames and Passwords” section of the Authentication Feature Overview and Configuration Guide).

**Examples**  To change the password to verySecurePassword, use the commands:
```
awplus# configure terminal
awplus(config)# auth-mac password verySecurePassword
```

**Validation Command**  `show running-config`

**Related Commands**  `auth two-step enable`
`show auth-mac`
**auth-mac reauth-relearning**

**Overview**  This command sets the MAC address learning of the supplicant (client device) to re-learning for re-authentication on the interface specified in the Interface command mode.

Use the **no** variant of this command to disable the auth-mac re-learning option.

**Syntax**  
```
auth-mac reauth-relearning
no auth-mac reauth-relearning
```

**Default**  Re-learning for port authentication is disabled by default.

**Mode**  Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples**  
To enable the re-authentication re-learning feature on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac reauth-relearning
```

To disable the re-authentication re-learning feature on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-mac reauth-relearning
```

**Validation Commands**
- `show auth-mac`
- `show auth-mac interface`
- `show running-config`
auth-web enable

**Overview**  
This command enables Web-based authentication in Interface mode on the interface specified.  
Use the no variant of this command to disable Web-based authentication on an interface.

**Syntax**  
auth-web enable  
no auth-web enable

**Default**  
Web-Authentication is disabled by default.

**Mode**  
Interface Configuration for a static channel or a switch port.

**Usage**  
Web-based authentication cannot be enabled if DHCP snooping is enabled (service dhcp-snooping command), and vice versa. You need to configure an IPv4 address for the VLAN interface on which Web Authentication is running.

**Examples**  
To enable Web-Authentication on static-channel-group 2, use the following commands:

```plaintext
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:

```plaintext
awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# static-channel-group 2  
awplus(config-if)# exit  
awplus(config)# interface sa2  
awplus(config-if)# no auth-web enable
```

**Validation Commands**

- show auth-web  
- show auth-web interface  
- show running-config

**Related Commands**

- aaa accounting auth-web default  
- aaa authentication auth-web
auth-web forward

**Overview**
This command enables the Web-Authentication packet forwarding feature on the interface specified. This command also enables ARP forwarding, and adds forwarded packets to the tcp or udp port number specified.

The **no** variant of this command disables or deletes the packet forwarding feature on the interface.

**Syntax**

```
auth-web forward [<ip-address>] {arp|dhcp|dns|tcp <1-65535>|udp <1-65535>}
no auth-web forward [<ip-address>] {arp|dhcp|dns|tcp <1-65535>|udp <1-65535>}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>Enable forwarding to the destination IPv4 address.</td>
</tr>
<tr>
<td>arp</td>
<td>Enable forwarding of ARP.</td>
</tr>
<tr>
<td>dhcp</td>
<td>Enable forwarding of DHCP (67/udp).</td>
</tr>
<tr>
<td>dns</td>
<td>Enable forwarding of DNS (53/udp).</td>
</tr>
<tr>
<td>tcp</td>
<td>Enable forwarding of TCP specified port number.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>TCP Port number.</td>
</tr>
<tr>
<td>udp</td>
<td>Enable forwarding of UDP specified port number.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>UDP Port number.</td>
</tr>
</tbody>
</table>

**Default**
Packet forwarding for port authentication is disabled by default.

**Mode**
Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage**
For more information about the `<ip-address>` parameter, and an example, see the "auth-web forward" section in the **Alliedware Plus Technical Tips and Tricks**.

**Examples**
To enable the ARP forwarding feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web forward arp
```
AUTHENTICATION COMMANDS

AUTH-WEB FORWARD

To add the TCP forwarding port 137 on interface port1.0.2, use the following commands:

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web forward tcp 137

To add the DNS Server IP address 192.168.1.10 on interface port1.0.2, use the following commands:

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth-web forward 192.168.1.10 dns

To disable the ARP forwarding feature on interface port1.0.2, use the following commands:

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward arp

To delete the TCP forwarding port 137 on interface port1.0.2, use the following commands:

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward tcp 137

To delete the all of TCP forwarding on interface port1.0.2, use the following commands:

awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward tcp

Validation Commands

show auth-web
show auth-web interface
show running-config
auth-web max-auth-fail

**Overview**  This command sets the number of authentication failures allowed before rejecting further authentication requests. When the supplicant (client device) fails more than has been set to the maximum number of authentication failures then login requests are refused during the quiet period.

The no variant of this command resets the maximum number of authentication failures to the default (three authentication failures).

**Syntax**  
```plaintext
auth-web max-auth-fail <0-10>
no auth-web max-auth-fail
```

**Default**  The `max-auth-fail` lock counter is set to three authentication failures by default.

**Mode**  Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples**  To set the lock count to 5 on interface port1.0.2, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web max-auth-fail 5
```

To set the lock count to the default on interface port1.0.2, use the following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web max-auth-fail
```

**Validation Commands**  
- `show auth-web`
- `show auth-web interface`
- `show running-config`

**Related Commands**  
- `auth timeout quiet-period`
auth-web method

**Overview**  This command sets the authentication method of Web-Authentication that is used with RADIUS on the interface specified.

The **no** variant of this command sets the authentication method to PAP for the interface specified when Web-Authentication is also used with the RADIUS authentication method.

**Syntax**  

```
auth-web method {eap-md5|pap}
```

```
no auth-web method
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eap-md5</td>
<td>Enable EAP-MDS as the authentication method.</td>
</tr>
<tr>
<td>pap</td>
<td>Enable PAP as the authentication method.</td>
</tr>
</tbody>
</table>

**Default**  The Web-Authentication method is set to PAP by default.

**Mode**  Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Example**  To set the Web-Authentication method to eap-md5 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web method eap-md5
```

**Validation Commands**  

- show auth-web
- show auth-web interface
- show running-config
auth-web-server blocking-mode

**Overview**  Use this command to enable blocking mode for the Web-Authentication server. The blocking mode displays an authentication success or failure screen immediately from the response result from a RADIUS server.

Use the no variant of this command to disable blocking mode for the Web-Authentication server.

**Syntax**

```plaintext
auth-web-server blocking-mode
no auth-web-server blocking-mode
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blocking-mode</td>
<td>Use blocking authentication server process.</td>
</tr>
<tr>
<td>no</td>
<td>Disable blocking mode.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
awplus# configure terminal
awplus(config)# auth-web-server blocking-mode
```

To disable blocking mode for the Web-Authentication server, use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# no auth-web-server blocking-mode
```

**Validation Commands**

- show running-config

**Related Commands**

- show auth-web-server
- auth-web-server mode (deleted)
- auth-web-server redirect-delay-time
auth-web-server dhcp ipaddress

**Overview**
Use this command to assign an IP address and enable the DHCP service on the Web-Authentication server for supplicants (client devices).

Use the `no` variant of this command to remove an IP address and disable the DHCP service on the Web-Authentication server for supplicants.

**Syntax**
```
auth-web-server dhcp ipaddress <ip-address/prefix-length>
nauth-web-server dhcp ipaddress
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-addr/prefix-length&gt;</code></td>
<td>The IPv4 address and prefix length assigned for the DHCP service on the Web-Authentication server for supplicants.</td>
</tr>
</tbody>
</table>

**Default**
No IP address for the Web-Authentication server is set by default.

**Mode**
Global Configuration

**Usage**
See the Authentication Feature Overview and Configuration Guide for information about:
- using DHCP with web authentication, and
- restrictions regarding combinations of authentication enhancements working together

**Examples**
To assign the IP address 10.0.0.1 to the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp ipaddress 10.0.0.1/8
```

To remove an IP address on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp ipaddress
```

**Validation Commands**
- `show running-config`

**Related Commands**
- `show auth-web-server`
- `auth-web-server dhcp lease`
AUTHENTICATION COMMANDS

AUTH-WEB-SERVER DHCP LEASE

auth-web-server dhcp lease

**Overview**

Use this command to set the DHCP lease time for supplicants (client devices) using the DHCP service on the Web-Authentication server.

Use the **no** variant of this command to reset to the default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server.

**Syntax**

```
auth-web-server dhcp lease <20-60>
no auth-web-server dhcp lease
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;20-60&gt;</td>
<td>DHCP lease time for supplicants using the DHCP service on the Web-Authentication server in seconds.</td>
</tr>
</tbody>
</table>

**Default**

The default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server is set to 30 seconds.

**Mode**

Global Configuration

**Usage**

See the Authentication Feature Overview and Configuration Guide for information about:

- using DHCP with web authentication, and
- restrictions regarding combinations of authentication enhancements working together

**Examples**

To set the DHCP lease time to 1 minute for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp lease 60
```

To reset the DHCP lease time to the default setting (30 seconds) for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp lease
```

**Validation Commands**

- show running-config

**Related Commands**

- show auth-web-server
- auth-web-server dhcp ipaddress
auth-web-server dhcp-wpad-option

**Overview** This command sets the DHCP WPAD (Web Proxy Auto-Discovery) option for the Web-Authentication temporary DHCP service.

For more information and examples, see the “Web Auth Proxy” section in the Alliedware Plus Technical Tips and Tricks.

Use the no variant of this command to disable the DHCP WPAD function.

**Syntax**

```
auth-web-server dhcp wpad-option <url>
no auth-web-server dhcp wpad-option
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;url&gt;</td>
<td>URL to the server which gets a .pac file.</td>
</tr>
</tbody>
</table>

**Default** The Web-Authentication server DHCP WPAD option is not set.

**Mode** Global Configuration

**Usage** If the supplicant is configured to use WPAD, the supplicant’s web browser will use TCP port 80 as usual. Therefore, the packet can be intercepted by Web-Authentication as normal, and the Web-Authentication Login page can be sent. However, after authentication, the browser does not know where to get the WPAD file and so cannot access external web pages. The WPAD file is usually named proxy.pac file and tells the browser what web proxy to use.

Use this command to tell the supplicant where it can get this file from. The switch itself can be specified as the source for this file, and it can deliver it to the supplicant on request.

**Example** To specify that the proxy.pac file is found on the server at 192.168.1.100, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp wpad-option
awplus(config)# http://192.168.1.100/proxy/proxy.pac
```

**Related Commands**

show auth-web-server
auth-web-server gateway (deleted)

**Overview**  This command has been deleted.
auth-web-server host-name

**Overview**  
This command assigns a hostname to the web authentication server.  
Use the **no** variant of this command to remove the hostname from the web authentication server.

**Syntax**  
auth-web-server host-name <hostname>  
no auth-web-server host-name

**Default**  
The web authentication server has no hostname.

**Mode**  
Global Configuration

**Usage**  
When the web authentication server uses HTTPS protocol, the web browser will validate the certificate. If the certificate is invalid, the web page gives a warning message before displaying server content. However, the web page will not give warning message if the server has a hostname same as the one stored in the installed certificate.

**Examples**  
To set the auth.example.com as the hostname of the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server host-name auth.example.com
```

To remove hostname auth.example.com from the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server host-name
```

**Related Commands**  
aaa authentication auth-mac  
auth-web enable
auth-web-server http-redirect (deleted)

**Overview**  This command has been deleted.
auth-web-server intercept-port

**Overview**  This command specifies any additional TCP port numbers that the Web-Authentication server is to intercept.

Use the no variant of this command to stop intercepting the TCP port numbers.

**Syntax**

```
auth-web-server intercept-port <1-65535>
no auth-web-server intercept-port <1-65535>
```

**Default**  No additional TCP port numbers are intercepted by default.

**Mode**  Global Configuration

**Usage**

If this command is not specified, AlliedWare Plus Web-Authentication intercepts the supplicant’s initial TCP port 80 connection to a web page and sends it the Web-Authentication Login page. However, if the supplicant is configured to use a web proxy, then it will usually be using TCP port 8080 (or another user configured port number). In this case Web-Authentication cannot intercept the connection.

To overcome this limitation you can now use this command to tell the switch which additional port it should intercept, and then send the Web-Authentication Login page to the supplicant.

When you use this command in conjunction with a proxy server configured in the web browser, you must add the proxy server’s network as a ‘No Proxy’ network. You can specify ‘No Proxy’ networks in the proxy settings in your web browser. For more information, see the “Web Auth Proxy” section in the Alliedware Plus Technical Tips and Tricks.

**Example**

To additionally intercept port number 3128, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server intercept-port 3128
```

**Related Commands**

- show auth-web-server
auth-web-server ipaddress

**Overview**  
This command sets the IP address for the Web-Authentication server. Use the no variant of this command to delete the IP address for the Web-Authentication server.

**Syntax**  
auth-web-server ipaddress <ip-address>

no auth-web-server ipaddress

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>Web-Authentication server dotted decimal IP address in A.B.C.D format.</td>
</tr>
</tbody>
</table>

**Default**  
The Web-Authentication server address on the system is not set by default.

**Mode**  
Global Configuration

**Examples**  
To set the IP address 10.0.0.1 to the Web-Authentication server, use the following commands:

awplus# configure terminal
awplus(config)# auth-web-server ipaddress 10.0.0.1

To delete the IP address from the Web-Authentication server, use the following commands:

awplus# configure terminal
awplus(config)# no auth-web-server ipaddress

**Validation Commands**
show auth-web
show auth-web-server
show running-config
**auth-web-server login-url**

**Overview**
This command sets the web-authentication login page URL. Use the `no` variant of this command to delete the set URL.

**Syntax**
- `auth-web-server login-url <URL>`
- `no auth-web-server login-url`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;URL&gt;</code></td>
<td>Set login page URL</td>
</tr>
</tbody>
</table>

**Default**
The built-in login page is set by default.

**Mode**
Global Configuration

**Examples**
To set `http://example.com/login.html` as the login page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server login-url
http://example.com/login.html
```

To unset the login page URL, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server login-url
```

**Validation Commands**
- `show running-config`
auth-web-server mode (deleted)

**Overview**  This command has been deleted.
auth-web-server page logo

**Overview**
This command sets the type of logo that will be displayed on the web authentication page.

Use the **no** variant of this command to set the logo type to **auto**.

**Syntax**
```
auth-web-server page logo {auto|default|hidden}
no auth-web-server page logo
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Display the custom logo if installed; otherwise display the default logo</td>
</tr>
<tr>
<td>default</td>
<td>Display the default logo</td>
</tr>
<tr>
<td>hidden</td>
<td>Hide the logo</td>
</tr>
</tbody>
</table>

**Default**
Logo type is **auto** by default.

**Mode**
Global Configuration

**Examples**
To display the default logo with ignoring installed custom logo, use the commands:
```
awplus# configure terminal
awplus(config)# auth-web-server page logo default
```

To set back to the default logo type **auto**, use the commands:
```
awplus# configure terminal
awplus(config)# no auth-web-server page logo
```

**Validation Commands**
`show auth-web-server page`
**auth-web-server page sub-title**

**Overview**  This command sets the custom sub-title on the web authentication page. Use the `no` variant of this command to reset the sub-title to its default.

**Syntax**

```
auth-web-server page sub-title {hidden|text <sub-title>}
no auth-web-server page sub-title
```

**Default**  “Allied-Telesis” is displayed by default.

**Mode**  Global Configuration

**Examples**

To set the custom sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title text Web Authentication
```

To hide the sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title hidden
```

To change back to the default title, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page sub-title
```

**Validation Commands**

```
show auth-web-server page
```
auth-web-server page success-message

**Overview**  This command sets the success message on the web-authentication page. Use the **no** variant of this command to remove the success message.

**Syntax**  

```
auth-web-server page success-message text <success-message>
no auth-web-server page success-message
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;success-message&gt;</code></td>
<td>Text string of the success message</td>
</tr>
</tbody>
</table>

**Default**  No success message is set by default.

**Mode**  Global Configuration

**Examples**  To set the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page success-message text Your success message
```

To unset the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page success-message
```

**Validation Commands**  show auth-web-server page
auth-web-server page title

**Overview**  This command sets the custom title on the web authentication page. Use the **no** variant of this command to remove the custom title.

**Syntax**  
```plaintext
auth-web-server page title {hidden|text <title>}
no auth-web-server page 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:
```plaintext
awplus# configure terminal
awplus(config)# auth-web-server page title text Login
```
To hide the title on the web authentication page, use the commands:
```plaintext
awplus# configure terminal
awplus(config)# auth-web-server page title hidden
```
To unset the custom title on the web authentication page, use the commands:
```plaintext
awplus# configure terminal
awplus(config)# no auth-web-server page title
```

**Validation Commands**  
show auth-web-server page
auth-web-server page welcome-message

**Overview**  
This command sets the welcome message on the web-authentication page. Use the `no` variant of this command to remove the welcome message.

**Syntax**  
```
auth-web-server page welcome-message text <welcome-message>
no auth-web-server page welcome-message
```

**Default**  
No welcome message is set by default.

**Mode**  
Global Configuration

**Examples**  
To set the welcome message on the web-authentication page, use the commands:
```
awplus# configure terminal
awplus(config)# auth-web-server page welcome-message text Your welcome message
```

To remove the welcome message on the web-authentication page, use the commands:
```
awplus# configure terminal
awplus(config)# no auth-web-server page welcome-message
```

**Validation Commands**  
```
show auth-web-server page
```
auth-web-server ping-poll enable

**Overview**
This command enables the ping polling to the supplicant (client device) that is authenticated by Web-Authentication.

The `no` variant of this command disables the ping polling to the supplicant that is authenticated by Web-Authentication.

**Syntax**
- `auth-web-server ping-poll enable`
- `no auth-web-server ping-poll enable`

**Default**
The ping polling feature for Web-Authentication is disabled by default.

**Mode**
Global Configuration

**Examples**
To enable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll enable
```

To disable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll enable
```

**Validation Commands**
- `show auth-web`
- `show auth-web-server`
- `show running-config`
auth-web-server ping-poll failcount

**Overview**  This command sets a fail count for the ping polling feature when used with Web-Authentication. The **failcount** parameter specifies the number of unanswered pings. A supplicant (client device) is logged off when the number of unanswered pings are greater than the failcount set with this command.

Use the **no** variant of this command to resets the fail count for the ping polling feature to the default (5 pings).

**Syntax**  
```
auth-web-server ping-poll failcount <1-100>
```
```
no auth-web-server ping-poll failcount
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-100&gt;</td>
<td>Count.</td>
</tr>
</tbody>
</table>

**Default**  The default failcount for ping polling is 5 pings.

**Mode**  Global Configuration

**Examples**  To set the failcount of ping polling to 10 pings, use the following commands:
```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll failcount 10
```
To set the failcount of ping polling to default, use the following commands:
```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll failcount
```

**Validation Commands**  
```
show auth-web
show auth-web-server
show running-config
```
auth-web-server ping-poll interval

**Overview**  This command is used to change the ping poll interval. The interval specifies the time period between pings when the supplicant (client device) is reachable.

Use the `no` variant of this command to reset to the default period for ping polling (30 seconds).

**Syntax**  
```
auth-web-server ping-poll interval <1-65535>
no auth-web-server ping-poll interval
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Seconds.</td>
</tr>
</tbody>
</table>

**Default**  The interval for ping polling is 30 seconds by default.

**Mode**  Global Configuration

**Examples**  To set the interval of ping polling to 60 seconds, use the following commands:
```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll interval 60
```

To set the interval of ping polling to the default (30 seconds), use the following commands:
```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll interval
```

**Validation Commands**  
- `show auth-web`
- `show auth-web-server`
- `show running-config`
AUTHENTICATION COMMANDS
AUTH-WEB-SERVER PING-POLL REAUTH-TIMER-REFRESH

auth-web-server ping-poll reauth-timer-refresh

**Overview**  This command modifies the reauth-timer-refresh parameter for the Web-Authentication feature. The reauth-timer-refresh parameter specifies whether a re-authentication timer is reset and when the response from a supplicant (a client device) is received.

Use the no variant of this command to reset the reauth-timer-refresh parameter to the default setting (disabled).

**Syntax**  
auth-web-server ping-poll reauth-timer-refresh  
no auth-web-server ping-poll reauth-timer-refresh

**Default**  The reauth-timer-refresh parameter is disabled by default.

**Mode**  Global Configuration

**Examples**  
To enable the reauth-timer-refresh timer, use the following commands:  
awplus# configure terminal  
awplus(config)# auth-web-server ping-poll reauth-timer-refresh  

To disable the reauth-timer-refresh timer, use the following commands:  
awplus# configure terminal  
awplus(config)# no auth-web-server ping-poll reauth-timer-refresh

**Validation Commands**  
show auth-web  
show auth-web-server  
show running-config
auth-web-server ping-poll timeout

**Overview**  This command modifies the ping poll *timeout* parameter for the Web-Authentication feature. The *timeout* parameter specifies the time in seconds to wait for a response to a ping packet.

Use the **no** variant of this command to reset the timeout of ping polling to the default (1 second).

**Syntax**  
auth-web-server ping-poll timeout <1-30>

no auth-web-server ping-poll timeout

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-30&gt;</td>
<td>Seconds.</td>
</tr>
</tbody>
</table>

**Default**  The default timeout for ping polling is 1 second.

**Mode**  Global Configuration

**Examples**  To set the timeout of ping polling to 2 seconds, use the command:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll timeout 2
```

To set the timeout of ping polling to the default (1 second), use the command:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll timeout
```

**Validation Commands**  
show auth-web
show auth-web-server
show running-config
auth-web-server port

**Overview**  This command sets the HTTP port number for the Web-Authentication server. Use the `no` variant of this command to reset the HTTP port number to the default (80).

**Syntax**

```
auth-web-server port <port-number>
no auth-web-server port
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;port-number&gt;</code></td>
<td>Set the local Web-Authentication server port within the TCP port number range 1 to 65535.</td>
</tr>
</tbody>
</table>

**Default**  The Web-Authentication server HTTP port number is set to 80 by default.

**Mode**  Global Configuration

**Examples**

To set the HTTP port number **8080** for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server port 8080
```

To reset to the default HTTP port number **80** for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server port
```

**Validation Commands**

- `show auth-web`
- `show auth-web-server`
- `show running-config`
auth-web-server redirect-delay-time

Overview  Use this command to set the delay time in seconds before redirecting the supplicant to a specified URL when the supplicant is authorized.

Use the variant `no` to reset the delay time set previously.

Syntax  

```
auth-web-server redirect-delay-time <5-60>
no auth-web-server redirect-delay-time
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redirect-delay-time</td>
<td>Set the delay time before jumping to a specified URL after the supplicant is authorized.</td>
</tr>
<tr>
<td>&lt;5-60&gt;</td>
<td>The time in seconds.</td>
</tr>
</tbody>
</table>

Default  The default redirect delay time is 5 seconds.

Mode  Global Configuration

Examples  To set the delay time to 60 seconds for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-delay-time 60
```

To reset the delay time, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-delay-time
```

Validation Command  

- `show auth-web-servers`
- `show running-config`

Related Commands  

- `auth-web-server redirect-url`
- `show auth-web-server`
**auth-web-server 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
```

**Default**
The redirect URL for the Web-Authentication server feature is not set by default (null).

**Mode**
Global Configuration

**Examples**
To enable and set redirect a URL string `www.alliedtelesis.com` for the Web-Authentication server, use the following commands:
```
awplus# configure terminal
awplus(config)# auth-web-server redirect-url http://www.alliedtelesis.com
```

To delete a redirect URL string, use the following commands:
```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-url
```

**Validation Commands**
- `show auth-web`
- `show auth-web-server`
- `show running-config`

**Related Commands**
- `auth-web-server http-redirect (deleted)`
- `auth-web-server redirect-delay-time`
**auth-web-server session-keep**

**Overview**  
This command enables the session-keep feature to jump to the original URL after being authorized by Web-Authentification.

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

**Syntax**  
```
auth-web-server session-keep
no auth-web-server session-keep
```

**Default**  
The session-keep feature is disabled by default.

**Mode**  
Global Configuration

**Usage**  
This function doesn't ensure to keep session information in all cases. Authenticated supplicant may be redirected to unexpected page when session-keep is enabled. This issue occurred by supplicant sending HTTP packets automatically after authentication page is displayed and the URL is written.

**Examples**  
To enable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server session-keep
```

To disable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server session-keep
```

**Validation Commands**  
- show auth-web
- show auth-web-server
- show running-config
AUTHENTICATION COMMANDS
AUTH-WEB-SERVER SSL

auth-web-server ssl

Overview
This command enables HTTPS functionality for the Web-Authentication server feature.

Use the no variant of this command to disable HTTPS functionality for the Web-Authentication server.

Syntax
auth-web-server ssl
no auth-web-server ssl

Default
HTTPS functionality for the Web-Authentication server feature is disabled by default.

Mode
Global Configuration

Examples
To enable HTTPS functionality for the Web-Authentication server feature, use the following commands:

awplus# configure terminal
awplus(config)# auth-web-server ssl

To disable HTTPS functionality for the Web-Authentication server feature, use the following commands:

awplus# configure terminal
awplus(config)# no auth-web-server ssl

Validation Commands
show auth-web
show auth-web-server
show running-config
auth-web-server sslport (deleted)

**Overview**  This command has been deleted.
auth-web-server ssl intercept-port

Overview
Use this command to register HTTPS intercept port numbers when the HTTPS server uses custom port number (not TCP port number 443).

Note that you need to use the auth-web-server intercept-port command to register HTTP intercept port numbers.

Use the no variant of this command to delete registered port number.

Syntax
auth-web-server ssl intercept-port <1-65535>
no auth-web-server ssl intercept-port <1-65535>

Parameter | Description
--- | ---
<1-65535> | TCP port number in the range from 1 through 65535

Default
443/TCP is registered by default.

Mode
Global Configuration

Examples
To register HTTPS port number 3128, use the commands:
```
awplus# configure terminal
awplus(config)# auth-web-server ssl intercept-port 3128
```

To delete HTTPS port number 3128, use the commands:
```
awplus# configure terminal
awplus(config)# no auth-web-server ssl intercept-port 3128
```

Validation
Commands
show auth-web-server

Related Commands
auth-web-server intercept-port
**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

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename&gt;</td>
<td>The URL of the PAC file.</td>
</tr>
</tbody>
</table>
**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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filename&gt;</code></td>
<td>The URL of the server certificate file.</td>
</tr>
</tbody>
</table>

**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`
**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
**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crc16l</td>
<td>The algorithm that will apply to the lower bits of CRC-16</td>
</tr>
<tr>
<td>crc16u</td>
<td>The algorithm that will apply to the upper bits of CRC-16</td>
</tr>
<tr>
<td>crc32l</td>
<td>The algorithm that will apply to the lower bits of CRC-32</td>
</tr>
<tr>
<td>crc32u</td>
<td>The algorithm that will apply to the upper bits of CRC-32</td>
</tr>
</tbody>
</table>

**Default**  
The hash-key algorithm is crc32l by default.

**Mode**  
Global configuration

**Usage**  
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.

A work-around when this situation occurs, can sometimes be applied 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.

**Syntax**
```
platform mac-vlan-hashing-algorithm
{crc16l|crc16u|crc32l|crc32u}
no platform mac-vlan-hashing-algorithm
```

**Default**
The hash-key algorithm is crc32l by default.

**Mode**
Global configuration

**Usage**
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.

A work-around when this situation occurs, can sometimes be applied 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crc16l</td>
<td>The algorithm that will apply to the lower bits of CRC-16</td>
</tr>
<tr>
<td>crc16u</td>
<td>The algorithm that will apply to the upper bits of CRC-16</td>
</tr>
<tr>
<td>crc32l</td>
<td>The algorithm that will apply to the lower bits of CRC-32</td>
</tr>
<tr>
<td>crc32u</td>
<td>The algorithm that will apply to the upper bits of CRC-32</td>
</tr>
</tbody>
</table>
show auth two-step supplicant brief

**Overview**
This command displays the supplicant state of the two-step authentication feature on the interface.

**Syntax**
```
show auth two-step supplicant [interface <ifrange>] brief
```

**Parameter**
- `interface <ifrange>`
The interface selected for display.
- `<ifrange>`
The interface types which can be specified as `<ifrange>`
  - Switch port (e.g. port1.0.6)
  - Static channel group (e.g. sa3)
  - Dynamic (LACP) channel group (e.g. po4)

**Mode**
Privileged Exec

**Usage**
Do not mix interface types in a list. The specified interfaces must exist.

**Example**
To display the supplicant state of the two-step authentication feature, enter the command:
```
awplus# show two-step supplicant interface port1.0.6 brief
```

**Output**
Figure 36-1: Example output from the show auth two-step supplicant brief command

```
interface port1.0.6
  authenticationMethod: dot1x/mac

  Two-Step Authentication:
  firstMethod:mac
  secondMethod:dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
  macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0
otherAuthenticationSupplicantNum: 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>VID</th>
<th>Mode</th>
<th>MAC Address</th>
<th>Status</th>
<th>FirstStep</th>
<th>SecondStep</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.6</td>
<td>1</td>
<td>D</td>
<td>000b..db67.00f7</td>
<td>Authenticated</td>
<td>Pass</td>
<td>Pass</td>
</tr>
</tbody>
</table>
```

**Related Commands**
- auth two-step enable
show auth-mac

**Overview**  This command shows authentication information for MAC-based authentication.

**Syntax**  `show auth-mac [all]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Display all authentication information for each interface available on the switch.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Example**  To display all MAC-based authentication information, enter the command:

```
awplus# show auth-mac all
```

**Output**  Figure 36-2: Example output from the `show auth-mac` command

```
802.1X Port-Based Authentication Disabled
MAC-based Port Authentication Enabled
WEB-based Port Authentication Disabled
```
show auth-mac diagnostics

**Overview**  This command shows MAC-Authentication diagnostics, optionally for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

**Syntax**  `show auth-mac diagnostics [interface <interface-list>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specify an interface to show</td>
</tr>
<tr>
<td>&lt;interface-list&gt;</td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• an interface (e.g. vlan2), a switch port (e.g. port1.0.6),</td>
</tr>
<tr>
<td></td>
<td>a static channel group (e.g. sa2) or a dynamic (LACP)</td>
</tr>
<tr>
<td></td>
<td>channel group (e.g. po2)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of interfaces, ports, static channel</td>
</tr>
<tr>
<td></td>
<td>groups or dynamic (LACP) channel groups separated by a</td>
</tr>
<tr>
<td></td>
<td>hyphen; e.g. vlan2-8, or port1.0.1-1.0.4, or sa1-2,</td>
</tr>
<tr>
<td></td>
<td>or po1-2</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above; e.g.</td>
</tr>
<tr>
<td></td>
<td>port1.0.1, port1.0.4-1.0.6. Do not mix interface types in</td>
</tr>
<tr>
<td></td>
<td>a list</td>
</tr>
</tbody>
</table>

The specified interfaces must exist.

**Mode**  Privileged Exec

**Example**  To display authentication diagnostics for port1.0.6, enter the command:

```
awplus# show auth-mac diagnostics interface port1.0.6
```

**Output**  Figure 36-3: Example output from the `show auth-mac diagnostics` command

```
Authentication Diagnostics for interface port1.0.6
Supplicant address: 00d0.59ab.7037
  authEnterConnecting: 2
  authEaplogoffWhileConnecting: 1
  authEnterAuthenticating: 2
  authSuccessWhileAuthenticating: 1
  authTimeoutWhileAuthenticating: 1
  authFailWhileAuthenticating: 0
  authEapstartWhileAuthenticating: 0
  authEaplogoffWhileAuthenticating: 0
  authReauthsWhileAuthenticated: 0
  authEapstartWhileAuthenticated: 0
  authEaplogoffWhileAuthenticated: 0
  BackendResponses: 2
  BackendAccessChallenges: 1
  BackendOtherrequestToSupplicant: 3
  BackendAuthSuccess: 1
```
show auth-mac interface

**Overview**

This command shows the status for MAC-based authentication on the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the optional `diagnostics` parameter to show authentication diagnostics for the specified interface. Use the optional `sessionstatistics` parameter to show authentication session statistics for the specified interface. Use the optional `statistics` parameter to show authentication diagnostics for the specified interface. Use the optional `supplicant` (client device) parameter to show the supplicant state for the specified interface.

**Syntax**

```
show auth-mac interface <interface-list>
[diagnostics|sessionstatistics|statistics|supplicant [brief]]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface-list&gt;</code></td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• an interface (e.g. <code>vlan2</code>), a switch port (e.g. <code>port1.0.6</code>), a static</td>
</tr>
<tr>
<td></td>
<td>channel group (e.g. <code>sa2</code>) or a dynamic (LACP) channel group (e.g. <code>po2</code>)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of interfaces, ports, static channel groups or dynamic</td>
</tr>
<tr>
<td></td>
<td>(LACP) channel groups separated by a hyphen; e.g. <code>vlan2-8</code>, or <code>port1.0.1-1.0.4</code>, or <code>sa1-2</code>, or <code>po1-2</code></td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above; e.g. <code>port1.0.1, port1.0.4-1.0.6</code>. Do</td>
</tr>
<tr>
<td></td>
<td>not mix interface types in a list</td>
</tr>
<tr>
<td>diagnostics</td>
<td>Diagnostics.</td>
</tr>
<tr>
<td>sessionstatistics</td>
<td>Session statistics.</td>
</tr>
<tr>
<td>statistics</td>
<td>Statistics.</td>
</tr>
<tr>
<td>supplicant</td>
<td>Supplicant (client device).</td>
</tr>
<tr>
<td>brief</td>
<td>Brief summary of supplicant state.</td>
</tr>
</tbody>
</table>

**Mode**

Privileged Exec

**Examples**

To display MAC-based authentication status for `port1.0.2`, enter the command:

```
awplus# show auth-mac interface port1.0.2
```

```
% Port-Control not configured on port1.0.2
```

To display MAC-Authentication diagnostics for `port1.0.2`, enter the command:

```
awplus# show auth-mac interface port1.0.2 diagnostics
```
AUTHENTICATION COMMANDS
SHOW AUTH-MAC INTERFACE

To display authentication session statistics for port1.0.6, enter the command:

```
awplus# show auth-mac interface port1.0.6 sessionstatistics
```

```
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
  authEaplogoffWhileAuthenticating: 0
  authReauthsWhileAuthenticated: 0
  authEapstartWhileAuthenticated: 0
  authEaplogoffWhileAuthenticated: 0
  BackendResponses: 2
  BackendAccessChallenges: 1
  BackendOtherrequestToSupplicant: 3
  BackendAuthSuccess: 1
```

To display MAC-Authentication statistics for port1.0.6 enter the command:

```
awplus# show auth-mac interface port1.0.6 statistics
```

To display the MAC authenticated supplicant on interface port1.0.6, enter the command:

```
awplus# show auth-mac interface port1.0.6 supplicant
```

Related Commands

- show auth-web diagnostics
- show dot1x sessionstatistics
- show dot1x statistics interface
- show dot1x supplicant interface
show auth-mac sessionstatistics

**Overview**  This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

**Syntax**  `show auth-mac sessionstatistics [interface <interface-list>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>Specify an interface to show.</td>
</tr>
<tr>
<td><code>&lt;interface-list&gt;</code></td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• an interface (e.g. <code>vlan2</code>), a switch port (e.g. <code>port1.0.6</code>),</td>
</tr>
<tr>
<td></td>
<td>a static channel group (e.g. <code>sa2</code>) or a dynamic (LACP) channel group</td>
</tr>
<tr>
<td></td>
<td>(e.g. <code>po2</code>)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of interfaces, ports, static channel groups or dynamic</td>
</tr>
<tr>
<td></td>
<td>(LACP) channel groups separated by a hyphen; e.g. <code>vlan2-8</code>, <code>port1.0.1-1.0.4</code>, <code>sa1-2</code>, <code>po1-2</code></td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above; e.g. <code>port1.0.1, port1.0.4-1.0.6</code>.</td>
</tr>
<tr>
<td></td>
<td>Do not mix interface types in a list.</td>
</tr>
<tr>
<td></td>
<td>The specified interfaces must exist.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Example**  To display output displaying MAC-Authentication session statistics for `port1.0.2`, enter the command:

```
awplus# show auth-mac sessionstatistics interface port1.0.2
```

**Output**  Figure 36-4: Example output from the `show auth-mac sessionstatistics` command

```
Authentication
session statistics for interface port1.0.2
  session user name: manager
    session authentication method: Remote server
    session time: 19440 secs
    session terminat cause: Not terminated yet
```
show auth-mac statistics interface

Overview
This command shows the authentication statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Syntax
show auth-mac statistics [interface <interface-list>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specify ports to show.</td>
</tr>
<tr>
<td>&lt;interface-list&gt;</td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• an interface (e.g. vlan2), a switch port (e.g. port1.0.6),</td>
</tr>
<tr>
<td></td>
<td>a static channel group (e.g. sa2) or a dynamic (LACP)</td>
</tr>
<tr>
<td></td>
<td>channel group (e.g. po2)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of interfaces, ports, static channel groups or</td>
</tr>
<tr>
<td></td>
<td>dynamic (LACP) channel groups separated by a hyphen; e.g.</td>
</tr>
<tr>
<td></td>
<td>vlan2-8, or port1.0.1-1.0.4, or</td>
</tr>
<tr>
<td></td>
<td>sa1-2, or po1-2</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above; e.g.</td>
</tr>
<tr>
<td></td>
<td>port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</td>
</tr>
<tr>
<td></td>
<td>The specified interfaces must exist.</td>
</tr>
</tbody>
</table>

Mode
Privileged Exec

Example
To display MAC-Authentication statistics for port1.0.2, enter the command:
awplus# show auth-mac statistics interface port1.0.2

Related Commands
show dot1x interface
show auth-mac supplicant

**Overview**  This command shows the supplicant (client device) state when MAC-Authentication is configured for the switch. This command shows a summary when the optional **brief** parameter is used.

**Syntax**  
```plaintext
show auth-mac supplicant [<macadd>] [brief]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;macadd&gt;</code></td>
<td>Mac (hardware) address of the Supplicant. Entry format is HHHH.HHHH.HHHH (hexadecimal).</td>
</tr>
<tr>
<td><strong>brief</strong></td>
<td>Brief summary of the Supplicant state.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Example**  To display the MAC authenticated supplicant for MAC address 00d0.59ab.7037, enter the command:

```
awplus# show auth-mac supplicant 00d0.59ab.7037
```

```
Web authentication server
  Server status: enabled
  Server address: -
  HTTP Port No: 80
  Security: enabled
  Certification: default
  SSL Port No: 443
  Redirect URL:
  Redirect Delay Time: 30
  HTTP Redirect: disabled
  Session keep: disabled
  PingPolling: disable
  PingInterval: 30
  Timeout: 1
  FailCount: 5
  ReauthFresh: disabled
```

To display a brief summary output for a MAC authenticated supplicant, enter the command:

```
awplus# show auth-mac supplicant brief
```

For example, if two-step authentication is configured with MAC-Authentication as the first method and 802.1X-Authentication as the second method then the output is as follows:
AUTHENTICATION COMMANDS

SHOW AUTH-MAC SUPPLICANT

For example, if two-step authentication is configured with MAC-Authentication as the first method and Web-Authentication as the second method then the output is as follows:

```
Interface port1.0.6
  authenticationMethod: dot1x/mac
  Two-Step Authentication
    firstMethod: mac
    secondMethod: dot1x
    totalSupplicantNum: 1
    authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    webBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0

  Interface   VID  Mode MAC Address    Status            IP Address      Username
  ============ ==== ==== ============== ================= ==============  =========
  port1.0.6   5    D    0008.0d5e.c216 Authenticated     --              dot1x
```

```
Interface port1.0.6
  authenticationMethod: mac/web
  Two-Step Authentication
    firstMethod: mac
    secondMethod: web
    totalSupplicantNum: 1
    authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 0
    webBasedAuthenticationSupplicantNum: 1
    otherAuthenticationSupplicantNum: 0

  Interface   VID  Mode MAC Address    Status            IP Address      Username
  ============ ==== ==== ============== ================= =============== =========
  port1.0.6   5    W    0008.0d5e.c216 Authenticated     192.168.1.200   web
```
show auth-mac supplicant interface

**Overview**  
This command shows the supplicant (client device) state for the MAC authenticated interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port. This command shows a summary when the optional `brief` parameter is used.

**Syntax**  
```
show auth-mac supplicant [interface <interface-list>] [brief]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specify ports to show.</td>
</tr>
</tbody>
</table>
| <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`, `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 MAC authenticated supplicant on the interface `port1.0.2`, enter the command:
```
awplus# show auth-mac supplicant interface port1.0.2
```
**show auth-web**

**Overview**  This command shows authentication information for Web-based authentication.

**Syntax**  show auth-web [all]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Example**  To display all Web-Authentication information, enter the command:

```
awplus# show auth-web all
```
AUTHENTICATION COMMANDS
SHOW AUTH-WEB

Output
Figure 36-5: Example output from the show auth-web command

awplus# show auth-web all
802.1X Port-Based Authentication Enabled
MAC-based Port Authentication Disabled
WEB-based Port Authentication Enabled
  RADIUS server address (auth): 150.87.17.192:1812
    Last radius message id: 4
Authentication Info for interface port1.0.1 portEnabled: true - portControl: Auto
portStatus: Authorized
reAuthenticate: disabled
reAuthPeriod: 3600
PAE: quietPeriod: 60 - maxReauthReg: 2 - txPeriod: 30
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in
KT: keyTxEnabled: false
critical: disabled
guestVlan: disabled
authFailVlan: disabled
dynamicVlanCreation: disabled
hostMode: single-host
dot1x: enabled
  protocolVersion: 1
authMac: disabled
authWeb: enabled
  method: PAP
  maxAuthFail: 3
  packetForwarding:
    10.0.0.1 80/tcp
dns
dhcp
twoStepAuthentication:
  configured: enabled
  actual: enabled
supplicantMac: none
Supplicant name: oha
  authenticationMethod: WEB-based Authentication
Two-Step Authentication:
  firstAuthentication: Pass - Method: dot1x
  secondAuthentication: Pass - Method: web
portStatus: Authorized - currentId: 3
PAE: state: Authenticated - portMode: Auto
PAE: reAuthCount: 0 - rxRespId: 0
PAE: quietPeriod: 60 - maxReauthReg: 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-mac
**show auth-web diagnostics**

**Overview**
This command shows Web-Authentication diagnostics, optionally for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

**Syntax**
```
show auth-web diagnostics [interface <interface-list>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specify ports to show.</td>
</tr>
<tr>
<td>&lt;interface-list&gt;</td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
</tbody>
</table>

- 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-web diagnostics interface port1.0.6
```

**Output**
Figure 36-6: Example output from the `show auth-web diagnostics` command

```
Authentication Diagnostics for interface port1.0.6
Supplicant address: 00d0.59ab.7037
  authEnterConnecting: 2
  authEaplogoffWhileConnecting: 1
  authEnterAuthenticating: 2
  authSuccessWhileAuthenticating: 1
  authTimeoutWhileAuthenticating: 1
  authFailWhileAuthenticating: 0
  authEapstartWhileAuthenticating: 0
  authEaplogoffWhileAuthenticated: 0
  authReauthsWhileAuthenticated: 0
  authEapstartWhileAuthenticated: 0
  authEaplogoffWhileAuthenticated: 0
  BackendResponses: 2
  BackendAccessChallenges: 1
  BackendOtherrequestToSupplicant: 3
  BackendAuthSuccess: 1
```
AUTHENTICATION COMMANDS
SHOW AUTH-WEB DIAGNOSTICS

**Related Commands**

- `show dot1x interface`
show auth-web interface

**Overview**  This command shows the status for Web based authentication on the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interface. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interface. Use the optional **statistics** parameter to show authentication diagnostics for the specified interface. Use the optional **supplicant** (client device) parameter to show the supplicant state for the specified interface.

**Syntax**  
```
show auth-web interface <interface-list> [diagnostics|sessionstatistics|statistics|supplicant [brief]]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-list&gt;</td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• an interface (e.g. vlan2), a switch port (e.g. port1.0.6),</td>
</tr>
<tr>
<td></td>
<td>a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g.</td>
</tr>
<tr>
<td></td>
<td>po2)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of interfaces, ports, static channel groups or</td>
</tr>
<tr>
<td></td>
<td>dynamic (LACP) channel groups separated by a hyphen; e.g. vlan2-8, or</td>
</tr>
<tr>
<td></td>
<td>port1.0.1-1.0.4, or sa1-2, or po1-2</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above; e.g.</td>
</tr>
<tr>
<td></td>
<td>port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</td>
</tr>
<tr>
<td></td>
<td>The specified interfaces must exist.</td>
</tr>
<tr>
<td>diagnostics</td>
<td>Diagnostics.</td>
</tr>
<tr>
<td>sessionstatistics</td>
<td>Session statistics.</td>
</tr>
<tr>
<td>statistics</td>
<td>Statistics.</td>
</tr>
<tr>
<td>supplicant</td>
<td>Supplicant (client device).</td>
</tr>
<tr>
<td>brief</td>
<td>Brief summary of supplicant state.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Example**  To display the Web based authentication status for port1.0.6, enter the command:

```
awplus# show auth-web interface port1.0.6
```

To display the Web based authentication status for port1.0.1, enter the command:

```
awplus# show auth-web interface port1.0.1
```
To display Web-Authentication diagnostics for port1.0.6, enter the command:

```
awplus# show auth-web interface port1.0.6 diagnostics
```

```
Authentication Info for interface port1.0.1
portEnabled: true  -  portControl: Auto
portStatus: Authorized
reAuthenticate: disabled
reAuthPeriod: 3600
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in
KT: keyTxEnabled: false
critical: disabled
guestVlan: disabled
authFailVlan: disabled
dynamicVlanCreation: disabled
hostMode: single-host
dot1x: enabled
  protocolVersion: 1
authMac: disabled
authWeb: enabled
  method: PAP
  maxAuthFail: 3
packetForwarding:
  10.0.0.1 80/tcp
dns
dhcp
twoStepAuthentication:
  configured: enabled
  actual: enabled
  supplicantMac: none
```

To display Web-Authentication session statistics for port1.0.6, enter the command:

```
awplus# show auth-web interface port1.0.6 sessionstatistics
```

```
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
  authEaplogoffWhileAuthenticated: 0
  authReauthsWhileAuthenticated: 0
  authEapstartWhileAuthenticated: 0
  authEaplogoffWhileAuthenticated: 0
BackendResponses: 2
BackendAccessChallenges: 1
BackendOtherRequestToSupplicant: 3
BackendAuthSuccess: 1
```

To display Web-Authentication session statistics for port1.0.6, enter the command:

```
awplus# show auth-web interface port1.0.6 sessionstatistics
```
AUTHENTICATION COMMANDS
SHOW AUTH-WEb INTERFACE

Authentication
session statistics for interface port1.0.6
    session user name: manager
    session authentication method: Remote server
    session time: 19440 secs
    session terminat cause: Not terminated yet

To display Web-Authentication statistics for port1.0.6, enter the command:
awplus# show auth-web statistics interface port1.0.6

To display the Web-Authenticated supplicant on interface port1.0.6, enter the command:
awplus# show auth-web interface port1.0.6 supplicant

Related Commands
show auth-web diagnostics
show dot1x sessionstatistics
show dot1x statistics interface
show dot1x supplicant interface
**show auth-web sessionstatistics**

**Overview**
This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

**Syntax**
```bash
show auth-web sessionstatistics [interface <interface-list>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>Specify ports to show.</td>
</tr>
<tr>
<td><code>&lt;interface-list&gt;</code></td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• an interface (e.g. <code>vlan2</code>), a switch port (e.g. <code>port1.0.6</code>), a static channel group (e.g. <code>sa2</code>) or a dynamic (LACP) channel group (e.g. <code>po2</code>)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. <code>vlan2-8</code>, or <code>port1.0.1-1.0.4</code>, or <code>sa1-2</code>, or <code>po1-2</code></td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above; e.g. <code>port1.0.1,port1.0.4-1.0.6</code>. Do not mix interface types in a list</td>
</tr>
<tr>
<td></td>
<td>The specified interfaces must exist.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
To display authentication statistics for `port1.0.6`, enter the command:

```
awplus# show auth-web sessionstatistics interface port1.0.6
```

**Output**
Figure 36-7: Example output from the `show auth-web sessionstatistics` command

```
Authentication session statistics for interface port1.0.6
  session user name: manager
  session authentication method: Remote server
  session time: 19440 secs
  session termination cause: Not terminated yet
```
**show auth-web statistics interface**

**Overview**  This command shows the authentication statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

**Syntax**  `show auth-web statistics interface <interface-list>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface-list&gt;</code></td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• an interface (e.g. <code>vlan2</code>), a switch port (e.g. <code>port1.0.6</code>), a static channel group (e.g. <code>sa2</code>) or a dynamic (LACP) channel group (e.g. <code>po2</code>)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. <code>vlan2-8</code>, <code>port1.0.1-1.0.4</code>, or <code>sa1-2</code>, or <code>po1-2</code></td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above; e.g. <code>port1.0.1,port1.0.4-1.0.6</code>. Do not mix interface types in a list</td>
</tr>
</tbody>
</table>

The specified interfaces must exist.

**Mode**  Privileged Exec

**Example**  To display Web-Authentication statistics for `port1.0.4`, enter the command:

```
awplus# show dot1x statistics interface port1.0.4
```

**Related Commands**  `show dot1x interface`
show auth-web supplicant

**Overview**  This command shows the supplicant (client device) state when Web-Authentication is configured for the switch. This command shows a summary when the optional `brief` parameter is used.

**Syntax**  show auth-web supplicant [<macadd>] [brief]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;macadd&gt;</code></td>
<td>Mac (hardware) address of the supplicant. Entry format is HHHH.HHHH.HHHH (hexadecimal).</td>
</tr>
<tr>
<td><code>brief</code></td>
<td>Brief summary of the supplicant state.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Examples**  To display Web authenticated supplicant information on the switch, enter the command:

`awplus# show auth-web supplicant`
show auth-web supplicant interface

**Overview**  This command shows the supplicant (client device) state for the Web authenticated interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port. This command shows a summary when the optional **brief** parameter is used.

**Syntax**  `show auth-web supplicant interface <interface-list> [brief]`

### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface-list&gt;</code></td>
<td>The interfaces or ports to configure. An interface-list can be:</td>
</tr>
<tr>
<td></td>
<td>• an interface (e.g. <code>vlan2</code>), a switch port (e.g. <code>port1.0.6</code>),</td>
</tr>
<tr>
<td></td>
<td>a static channel group (e.g. <code>sa2</code>) or a dynamic (LACP) channel group</td>
</tr>
<tr>
<td></td>
<td>(e.g. <code>po2</code>)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of interfaces, ports, static channel groups or dynamic</td>
</tr>
<tr>
<td></td>
<td>(LACP) channel groups separated by a hyphen; e.g. <code>vlan2-8</code>, <code>orport1.0.1-1.0.4</code>, <code>or sa1-2</code>, <code>or po1-2</code></td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of the above; e.g. <code>port1.0.1, port1.0.4-1.0.6</code>.</td>
</tr>
<tr>
<td></td>
<td>Do not mix interface types in a list.</td>
</tr>
<tr>
<td><strong>brief</strong></td>
<td>Brief summary of the supplicant state.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Examples**  To display the Web authenticated supplicant on the interface `port1.0.3`, enter the command:

```
awplus# show auth-web supplicant interface port1.0.3
```

To display brief summary output for the Web authenticated supplicant, enter the command:

```
awplus# show auth-web supplicant brief
```
show auth-web-server

**Overview**  
This command shows the Web-Authentication server configuration and status on the switch.

**Syntax**  
show auth-web-server

**Mode**  
Privileged Exec

**Example**  
To display Web-Authentication server configuration and status, enter the command:

```
awplus# show auth-web-server
```

**Output**  
Figure 36-8: Example output from the `show auth-web-server` command

```
Web authentication server
 Server status: enabled
 Server mode: none
 Server address: 192.168.1.1/24
   DHCP server enabled
   DHCP lease time: 20
   DHCP WPAD Option URL: http://192.168.1.1/proxy.pac
 HTTP Port No: 80
 Security: disabled
 Certification: default
 SSL Port No: 443
 Redirect URL: --
 Redirect Delay Time: 5
 HTTP Redirect: enabled
 Session keep: disabled
 PingPolling: disabled
 PingInterval: 30
 Timeout: 1
 FailCount: 5
 ReauthTimerRefresh: disabled
```

**Related Commands**

- auth-web-server gateway (deleted)
- auth-web-server http-redirect (deleted)
- auth-web-server ipaddress
- auth-web-server port
- auth-web-server redirect-delay-time
- auth-web-server redirect-url
- auth-web-server session-keep
- auth-web-server ssl
- auth-web-server sslport (deleted)
show auth-web-server page

**Overview**  This command displays the web-authentication page configuration and status.

**Syntax**  show auth-web-server page

**Mode**  Privileged Exec

**Examples**  To show the web-authentication page information, use the command:

```
awplus# show auth-web-server page
```

Table 36-1: Example output from the show auth-web-server page command on the console.

```
awplus#show auth-web-server page
Web authentication page
  Logo: auto
  Title: default
  Sub-Title: Web Authentication
  Welcome message: Your welcome message
  Success message: Your success message
```

**Related Commands**  auth-web forward

auth-web-server page logo

auth-web-server page sub-title

auth-web-server page success-message

auth-web-server page title

auth-web-server page welcome-message
show proxy-autoconfig-file

**Overview**  
This command displays the contents of the proxy auto configuration (PAC) file.

**Syntax**  
show proxy-autoconfig-file

**Mode**  
Privileged Exec

**Example**  
To display the contents of the proxy auto configuration (PAC) file, enter the command:

```
awplus# show auth proxy-autoconfig-file
```

**Output**  
Figure 36-9: Example output from the show proxy-autoconfig-file

```
function FindProxyForURL(url,host)
{
    if (isPlainHostName(host) ||
        isInNet(host, ”192.168.1.0”,”255.255.255.0”)) {
        return ”DIRECT”;
    }
    else {
        return ”PROXY 192.168.110.1:8080”;
    }
}
```

**Related Commands**

- copy proxy-autoconfig-file
- erase proxy-autoconfig-file
Introduction

Overview  This chapter provides an alphabetical reference for AAA commands for Authentication, Authorization and Accounting. For more information, see the AAA Feature Overview and Configuration Guide.
AAA COMMANDS

Command List

- “aaa accounting auth-mac default” on page 1617
- “aaa accounting auth-web default” on page 1619
- “aaa accounting commands” on page 1621
- “aaa accounting dot1x” on page 1623
- “aaa accounting login” on page 1625
- “aaa accounting update” on page 1628
- “aaa authentication auth-mac” on page 1630
- “aaa authentication auth-web” on page 1631
- “aaa authentication dot1x” on page 1632
- “aaa authentication enable default group tacacs+” on page 1633
- “aaa authentication enable default local” on page 1635
- “aaa authentication login” on page 1636
- “aaa group server” on page 1638
- “aaa local authentication attempts lockout-time” on page 1640
- “aaa local authentication attempts max-fail” on page 1641
- “accounting login” on page 1642
- “clear aaa local user lockout” on page 1643
- “debug aaa” on page 1644
- “login authentication” on page 1645
- “show aaa local user locked” on page 1646
- “show debugging aaa” on page 1647
- “undebug aaa” on page 1648
aaa accounting auth-mac default

**Overview**
This command configures a default accounting method list for MAC-based Authentication. The default accounting method list specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting method list is automatically applied to interfaces with MAC-based Authentication enabled.

Use the `no` variant of this command to disable AAA accounting for MAC-based Authentication globally.

**Syntax**
```
aaa accounting auth-mac default {start-stop|stop-only|none} group {<group-name>|radius}
no aaa accounting auth-mac default
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start-stop</td>
<td>Start and stop records to be sent.</td>
</tr>
<tr>
<td>stop-only</td>
<td>Stop records to be sent.</td>
</tr>
<tr>
<td>none</td>
<td>No accounting record to be sent.</td>
</tr>
<tr>
<td>&lt;group-name&gt;</td>
<td>Server group name.</td>
</tr>
<tr>
<td>radius</td>
<td>Use all RADIUS servers</td>
</tr>
</tbody>
</table>

**Default**
RADIUS accounting for MAC-based Authentication is disabled by default

**Mode**
Global Configuration

**Usage**
There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by `radius-server host` command
- **group <group-name>**: use the specified RADIUS server group configured with the `aaa group server` command

The accounting event to send to the RADIUS server is configured with the following options:

- **start-stop**: sends a `start` accounting message at the beginning of a session and a `stop` accounting message at the end of the session.
- **stop-only**: sends a `stop` accounting message at the end of a session.
- **none**: disables accounting.

Use the `no` variant of this command to disable AAA accounting for MAC-based Authentication globally.
AAA ACCOUNTING AUTH-MAC DEFAULT

**Examples**

To enable RADIUS accounting for MAC-based Authentication, and use all available RADIUS Servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-mac default start-stop
group radius
```

To disable RADIUS accounting for MAC-based Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-mac default
```

**Related Commands**

`aaa authentication auth-mac`
aaa accounting auth-web default

**Overview**
This command configures a default accounting method list for Web-based Port Authentication. The default accounting method list specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting method list is automatically applied to interfaces with Web-based Authentication enabled.

Use the `no` variant of this command to disable AAA accounting for Web-based Port Authentication globally.

**Syntax**
`aaa accounting auth-web default {start-stop|stop-only|none} group {<group-name>|radius}
no aaa accounting auth-web default`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start-stop</td>
<td>Start and stop records to be sent.</td>
</tr>
<tr>
<td>stop-only</td>
<td>Stop records to be sent.</td>
</tr>
<tr>
<td>none</td>
<td>No accounting record to be sent.</td>
</tr>
<tr>
<td>&lt;group-name&gt;</td>
<td>Server group name.</td>
</tr>
<tr>
<td>radius</td>
<td>Use all RADIUS servers.</td>
</tr>
</tbody>
</table>

**Default**
RADIUS accounting for Web-based Port Authentication is disabled by default.

**Mode**
Global Configuration

**Usage**
There are two ways to define servers where RADIUS accounting messages are sent:
- `group radius`: use all RADIUS servers configured by `radius-server host` command
- `group <group-name>`: use the specified RADIUS server group configured with the `aaa group server` command

Configure the accounting event to be sent to the RADIUS server with the following options:
- `start-stop`: sends a `start` accounting message at the beginning of a session and a `stop` accounting message at the end of the session.
- `stop-only`: sends a `stop` accounting message at the end of a session.
- `none`: disables accounting.

**Examples**
To enable RADIUS accounting for Web-based Authentication, and use all available RADIUS Servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-web default start-stop group radius
```
To disable RADIUS accounting for Web-based Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-web default
```

**Related Commands**

`aaa authentication auth-web`
AAA COMMANDS
AAA ACCOUNTING COMMANDS

aaa accounting commands

**Overview**
Use this command to configure and enable TACACS+ command accounting. When command accounting is enabled, information about a command entered at a specified privilege level on a device is sent to a TACACS+ server. To account for all commands entered on a device you need to configure command accounting for each discrete privilege level. A command accounting record includes the command as entered for the specified privilege level, the date and time each command execution finished, and the username of the user who executed the command.

This command creates a default method list that is applied to every console and vty line. The **stop-only** parameter indicates that an accounting message is sent to the TACACS+ server when a command has stopped executing.

Note that up to four TACACS+ servers can be configured for accounting. The servers are checked for reachability in the order they are configured and only the first reachable server is used. If no server is found the accounting message is dropped.

Use the **no** variant of this command to disable command accounting.

**Syntax**
```
aaa accounting commands <1-15> default stop-only group tacacs+
no aaa accounting commands <1-15> default
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-15&gt;</td>
<td>The privilege level, in the range 1 to 15.</td>
</tr>
</tbody>
</table>

**Default**
TACACS+ command accounting is disabled by default.

**Mode**
Global Configuration

**Usage**
When command accounting is enabled, the command as entered is included in the accounting packets sent to the TACACS+ accounting server.

You cannot enable command accounting if a trigger is configured. An error message is displayed if you attempt to enable command accounting and a trigger is configured.

The **show tech-support** command runs a number of commands and each command is accounted separately.

When the **copy <filename> running-config** command is executed all the commands of a configuration file copied into the running-config are accounted separately.
AAA ACCOUNTING COMMANDS

Examples

To configure command accounting for privilege level 15 commands, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting commands 15 default stop-only group tacacs+
```

To disable command accounting for privilege level 15 commands, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting commands 15 default
```

Related Commands

aaa authentication login
aaa accounting login
accounting login
tacacs-server host
aaa accounting dot1x

**Overview**  
This command configures the default accounting method list for IEEE 802.1X-based Authentication. The default accounting method list specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting method list is automatically applied to interfaces with IEEE 802.1X-based Authentication enabled.

Use the `no` variant of this command to disable AAA accounting for 802.1X-based Port Authentication globally.

**Syntax**  
```
aaa accounting dot1x default {start-stop|stop-only|none} group {<group-name>|radius}
no aaa accounting dot1x default
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start-stop</td>
<td>Start and stop records to be sent.</td>
</tr>
<tr>
<td>stop-only</td>
<td>Stop records to be sent.</td>
</tr>
<tr>
<td>none</td>
<td>No accounting record to be sent.</td>
</tr>
<tr>
<td>&lt;group-name&gt;</td>
<td>Server group name.</td>
</tr>
<tr>
<td>radius</td>
<td>Use all RADIUS servers.</td>
</tr>
</tbody>
</table>

**Default**  
RADIUS accounting for 802.1X-based Port Authentication is disabled by default (there is no default server set by default).

**Mode**  
Global Configuration

**Usage**  
There are two ways to define servers where RADIUS accounting messages will be sent:

- `group radius` : use all RADIUS servers configured by `radius-server host` command.
- `group <group-name>` : use the specified RADIUS server group configured with the `aaa group server` command.

The accounting event to send to the RADIUS server is configured by the following options:

- `start-stop` : sends a `start` accounting message at the beginning of a session and a `stop` accounting message at the end of the session.
- `stop-only` : sends a `stop` accounting message at the end of a session.
- `none` : disables accounting.
### Examples

To enable RADIUS accounting for 802.1X-based Authentication, and use all available RADIUS Servers, use the commands:

```bash
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:

```bash
awplus# configure terminal
awplus(config)# no aaa accounting dot1x default
```

### Related Commands

- `aaa accounting update`
- `aaa authentication dot1x`
- `aaa group server`
- `dot1x port-control`
- `radius-server host`
aaa accounting login

**Overview**  This command configures RADIUS and TACACS+ accounting for login shell sessions. The specified method list name can be used by the `accounting login` command in the Line Configuration mode. If the `default` parameter is specified, then this creates a default method list that is applied to every console and vty line, unless another accounting method list is applied on that line.

Note that unlimited RADIUS servers and up to four TACACS+ servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the `no` variant of this command to remove an accounting method list for login shell sessions configured by an `aaa accounting login` command. If the method list being deleted is already applied to a console or vty line, accounting on that line will be disabled. If the default method list name is removed by this command, it will disable accounting on every line that has the default accounting configuration.

**Syntax**

```plaintext
aaa accounting login
{default|<list-name>}{start-stop|stop-only|none} {group
{radius|tacacs+|<group-name>}}
no aaa accounting login {default|<list-name>}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Default accounting method list.</td>
</tr>
<tr>
<td>&lt;list-name&gt;</td>
<td>Named accounting method list.</td>
</tr>
<tr>
<td>start-stop</td>
<td>Start and stop records to be sent.</td>
</tr>
<tr>
<td>stop-only</td>
<td>Stop records to be sent.</td>
</tr>
<tr>
<td>none</td>
<td>No accounting record to be sent.</td>
</tr>
<tr>
<td>group</td>
<td>Specify the servers or server group where accounting packets are sent.</td>
</tr>
<tr>
<td>radius</td>
<td>Use all RADIUS servers configured by the <code>radius-server host</code> command.</td>
</tr>
<tr>
<td>tacacs+</td>
<td>Use all TACACS+ servers configured by the <code>tacacs-server host</code> command.</td>
</tr>
<tr>
<td>&lt;group-name&gt;</td>
<td>Use the specified RADIUS server group, as configured by the <code>aaa group server</code> command.</td>
</tr>
</tbody>
</table>

**Default**  Accounting for login shell sessions is disabled by default.

**Mode**  Global Configuration
**Usage**

This command enables you to define a named accounting method list. The items that you define in the accounting options are:

- the types of accounting packets that will be sent
- the set of servers to which the accounting packets will be sent

You can define a default method list with the name `default` and any number of other named method lists. The `<list-name>` for any method list that you define can then be used as the `<list-name>` parameter in the `accounting login` command available from Line Configuration mode.

If the method list name already exists, the command will replace the existing configuration with the new one.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by `radius-server host` command
- **group <group-name>**: use the specified RADIUS server group configured with the `aaa group server` command

There is one way to define servers where TACACS+ accounting messages are sent:

- **group tacacs+**: use all TACACS+ servers configured by `tacacs-server host` command

The accounting event to send to the RADIUS or TACACS+ server is configured with the following options:

- **start-stop**: sends a `start` accounting message at the beginning of a session and a `stop` accounting message at the end of the session.
- **stop-only**: sends a `stop` accounting message at the end of a session.
- **none**: disables accounting.

**Examples**

To configure RADIUS accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group radius
```

To configure TACACS+ accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group tacacs+
```

To reset the configuration of the default accounting list, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting login default
```
AAA ACCOUNTING LOGIN

**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
```

**Default**  Periodic accounting update is disabled by default.

**Mode**  Global Configuration

**Usage**  Use this command to enable the device to send periodic AAA login accounting reports to the accounting server. When periodic accounting report is enabled, interim accounting records are sent according to the interval specified by the `periodic` parameter. The accounting updates are start messages.

If the `no` variant of this command is used to disable periodic accounting reporting, any interval specified by the `periodic` parameter is reset to the default of 30 minutes when accounting reporting is reenabled, unless this interval is specified.

**Examples**  To configure the switch to send period accounting updates every 30 minutes, the default period, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update
```

To configure the switch to send period accounting updates every 10 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update periodic 10
```
AAA COMMANDS
AAA ACCOUNTING UPDATE

To disable periodic accounting update wherever accounting has been configured, use the following commands:

awplus# configure terminal
awplus(config)# no aaa accounting update

Related Commands

aaa accounting auth-mac default
aaa accounting auth-web default
aaa accounting dot1x
aaa accounting login
aaa authentication auth-mac

### Overview
This command enables MAC-based Port Authentication globally and allows you to specify an authentication method list. It is automatically applied to every interface running MAC-based Port Authentication.

Use the **no** variant of this command to globally disable MAC-based Port Authentication.

### Syntax
```
aaa authentication auth-mac default group {<group-name>|radius}
no aaa authentication auth-mac default
```

### Default
MAC-based Port Authentication is disabled by default.

### Mode
Global Configuration

### Usage
There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by `radius-server host` command
- **group <group-name>**: use the specified RADIUS server group configured with the `aaa group server` command

All configured RADIUS Servers are automatically members of the server group `radius`. If a server is added to a named group `<group-name>`, it also remains a member of the group `radius`.

### Examples
To enable MAC-based Port Authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-mac default group radius
```

To disable MAC-based Port Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-mac default
```

### Related Commands
- `aaa accounting auth-mac default`
- `auth-mac enable`
aaa authentication auth-web

Overview
This command enables Web-based Port Authentication globally and allows you to enable an authentication method list (in this case, a list of RADIUS Servers). It is automatically applied to every interface running Web-based Port Authentication.

Use the no variant of this command to globally disable Web-based Port Authentication.

Syntax
```
aaa authentication auth-web default group {<group-name>|radius}
```
```
no aaa authentication auth-web default
```

Default
Web-based Port Authentication is disabled by default.

Mode
Global Configuration

Usage
There are two ways to define servers where RADIUS accounting messages are sent:

- `group radius`: use all RADIUS servers configured by `radius-server host` command
- `group <group-name>`: use the specified RADIUS server group configured with the `aaa group server` command

Note that you need to configure an IPv4 address for the VLAN interface on which We Authentication is running.

Examples
To enable Web-based Port Authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:
```
awplus# configure terminal
awplus(config)# aaa authentication auth-web default group radius
```

To disable Web-based Port Authentication, use the commands:
```
awplus# configure terminal
awplus(config)# no aaa authentication auth-web default
```

Related Commands
- `aaa accounting auth-web default`
- `auth-mac enable`
aaa authentication dot1x

**Overview**
This command enables 802.1X-based Port Authentication globally and allows you to enable an authentication method list. It is automatically applied to every interface running 802.1X-based Port Authentication.

Use the `no` variant of this command to globally disable 802.1X-based Port Authentication.

**Syntax**
```
aaa authentication dot1x default group {<group-name>|radius}
no aaa authentication dot1x default
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius</td>
<td>Use all RADIUS servers.</td>
</tr>
<tr>
<td>&lt;group-name&gt;</td>
<td>Server group name.</td>
</tr>
</tbody>
</table>

**Default**
802.1X-based Port Authentication is disabled by default.

**Mode**
Global Configuration

**Usage**
Use this command to specify the default method list to use for authentication on all switch ports with 802.1X enabled. Use the `no` variant of this command to reset the authentication method list for 802.1X to its default (i.e. to use the group `radius`, containing all RADIUS servers configured by the `radius-server host` command).

There are two ways to define servers where RADIUS accounting messages are sent:

- `group radius`: use all RADIUS servers configured by `radius-server host` command
- `group <group-name>`: use the specified RADIUS server group configured with the `aaa group server` command

**Examples**
To enable 802.1X-based Port Authentication globally with all RADIUS servers, and use all available RADIUS servers, use the command:
```
awplus# configure terminal
awplus(config)# aaa authentication dot1x default group radius
```

To disable 802.1X-based Port Authentication, use the command:
```
awplus# configure terminal
awplus(config)# no aaa authentication dot1x default
```

**Related Commands**
- `aaa accounting dot1x`
- `aaa group server`
- `dot1x port-control`
- `radius-server host`
aaa authentication enable default group tacacs+

**Overview**
This command enables AAA authentication to determine the privilege level a user can access for passwords authenticated against the TACACS+ server.

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

**Syntax**
```bash
aaa authentication enable default group tacacs+ [local] [none]
no aaa authentication enable default
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>local</strong></td>
<td>Use the locally configured enable password (<strong>enable password</strong> command) for authentication.</td>
</tr>
<tr>
<td><strong>none</strong></td>
<td>No authentication.</td>
</tr>
</tbody>
</table>

**Default**
Local privilege level authentication is enabled by default (**aaa authentication enable default local** command).

**Mode**
Global Configuration

**Usage**
A user is configured on a TACACS+ server with a maximum privilege level. When they enter the **enable (Privileged Exec mode)** command they are prompted for an enable password which is authenticated against the TACACS+ server. If the password is correct and the specified privilege level is equal to or less than the users maximum privilege level, then they are granted access to that level. If the user attempts to access a privilege level that is higher than their maximum configured privilege level, then the authentication session will fail and they will remain at their current privilege level.

**NOTE:** *If both local and none are specified, you must always specify local first.*

If the TACACS+ server goes offline, or is not reachable during enable password authentication, and command level authentication is configured as:

- **aaa authentication enable default group tacacs+**
  then the user is never granted access to Privileged Exec mode.

- **aaa authentication enable default group tacacs+ local**
  then the user is authenticated using the locally configured enable password, which if entered correctly grants the user access to Privileged Exec mode. If no enable password is locally configured (**enable password** command),
then the enable authentication will fail until the TACACS+ server becomes available again.

- **aaa authentication enable default group tacacs+ none**
  then the user is granted access to Privileged Exec mode with no authentication. This is true even if a locally configured enable password is configured.

- **aaa authentication enable default group tacacs+ local none**
  then the user is authenticated using the locally configured enable password. If no enable password is locally configured, then the enable authentication will grant access to Privileged Exec mode with no authentication.

If the password for the user is not successfully authenticated by the server, then the user is again prompted for an enable password when they enter **enable** via the CLI.

### Examples
To enable a privilege level authentication method that will not allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default group tacacs+
```

To enable a privilege level authentication method that will allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, and a locally configured enable password is configured, use the following commands:

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

To disable privilege level authentication, use the following commands:

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

### Related Commands
- **aaa authentication login**
- **aaa authentication enable default local**
- **enable (Privileged Exec mode)**
- **enable password**
- **enable secret**
- **tacacs-server host**
aaa authentication enable default local

**Overview**
This command enables AAA authentication to determine the privilege level a user can access for passwords authenticated locally.

**Syntax**
```
aaa authentication enable default local
```

**Default**
Local privilege level authentication is enabled by default.

**Mode**
Global Configuration

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

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

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

To disable privilege level authentication, use the following commands:

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

**Related Commands**
- aaa authentication enable default group tacacs+
- aaa authentication login
- `enable (Privileged Exec mode)`
- `enable password`
- `enable secret`
- `tacacs-server host`
aaa authentication login

**Overview**  Use this command to create an ordered list of methods to use to authenticate user login, or to replace an existing method list with the same name. Specify one or more of the options `local` or `group`, in the order you want them to be applied. If the default method list name is specified, it is applied to every console and VTY line immediately unless another method list is applied to that line by the `login authentication` command. To apply a non-default method list, you must also use the `login authentication` command.

Use the `no` variant of this command to remove an authentication method list for user login. The specified method list name is deleted from the configuration. If the method list name has been applied to any console or VTY line, user login authentication on that line will fail.

Note that the `no aaa authentication login default` command does not remove the default method list. This will return the default method list to its default state (`local` is the default).

**Syntax**

```
aaa authentication login {default|<list-name>} {{local} [group {radius|tacacs+}<group-name>]]
no aaa authentication login {default|<list-name>}
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Set the default authentication server for user login.</td>
</tr>
<tr>
<td><code>&lt;list-name&gt;</code></td>
<td>Name of authentication server.</td>
</tr>
<tr>
<td><code>local</code></td>
<td>Use the local username database.</td>
</tr>
<tr>
<td><code>group</code></td>
<td>Use server group.</td>
</tr>
<tr>
<td><code>radius</code></td>
<td>Use all RADIUS servers configured by the <code>radius-server host</code> command.</td>
</tr>
<tr>
<td><code>tacacs+</code></td>
<td>Use all TACACS+ servers configured by the <code>tacacs-server host</code> command.</td>
</tr>
<tr>
<td><code>&lt;group-name&gt;</code></td>
<td>Use the specified RADIUS server group, as configured by the <code>aaa group server</code> command.</td>
</tr>
</tbody>
</table>

**Default**  If the default server is not configured using this command, user login authentication uses the local user database only.

If the `default` method list name is specified, it is applied to every console and VTY line immediately unless a named method list server is applied to that line by the `login authentication` command.

`local` is the default state for the default method list unless a named method list is applied to that line by the `login authentication` command. Reset to the default method list using the `no aaa authentication login default` command.

**Mode**  Global Configuration
AAA COMMANDS
AAA AUTHENTICATION LOGIN

Usage
When a user attempts to log in, the switch sends an authentication request to the first authentication server in the method list. If the first server in the list is reachable and it contains a username and password matching the authentication request, the user is authenticated and the login succeeds. If the authentication server denies the authentication request because of an incorrect username or password, the user login fails. If the first server in the method list is unreachable, the switch sends the request to the next server in the list, and so on.

For example, if the method list specifies group tacacs+ local, and a user attempts to log in with a password that does not match a user entry in the first TACACS+ server, if this TACACS+ server denies the authentication request, then the switch does not try any other TACACS+ servers not the local user database; the user login fails.

Examples
To configure the default authentication method list for user login to first use all available RADIUS servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login default group radius local
```

To configure a user login authentication method list called USERS to first use the RADIUS server group RAD_GROUP1 for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group RAD_GROUP1 local
```

To configure a user login authentication method list called USERS to first use the TACACS+ servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group tacacs+ local
```

To return to the default method list (local is the default server), use the following commands:

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

To delete an existing authentication method list USERS created for user login authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication login USERS
```

Related Commands
- aaa accounting commands
- aaa authentication enable default group tacacs+
- login authentication
aaa group server

**Overview**  This command configures a RADIUS server group. A server group can be used to specify a subset of RADIUS servers in `aaa` commands. The group name `radius` is predefined, which includes all RADIUS servers configured by the `radius-server host` command.

RADIUS servers are added to a server group using the `server` command. Each RADIUS server should be configured using the `radius-server host` command.

Use the `no` variant of this command to remove an existing RADIUS server group.

**Syntax**
```
aaa group server radius <group-name>
no aaa group server radius <group-name>
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;group-name&gt;</code></td>
<td>Server group name.</td>
</tr>
</tbody>
</table>

**Mode**  Global Configuration

**Usage**  Use this command to create an AAA group of RADIUS servers, and to enter Server Group Configuration mode, in which you can add servers to the group. Use a server group to specify a subset of RADIUS servers in AAA commands. Each RADIUS server must be configured by the `radius-server host` command. To add RADIUS servers to a server group, use the `server` command.

**Examples**  To create a RADIUS server group named GROUP1 with hosts 192.168.1.1, 192.168.2.1 and 192.168.3.1, use the commands:
```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.2.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.3.1 auth-port 1812 acct-port 1813
```

To remove a RADIUS server group named GROUP1 from the configuration, use the command:
```
awplus(config)# no aaa group server radius GROUP1
```
AAA COMMANDS

AAA GROUP SERVER

Related Commands

aaa accounting auth-mac default
aaa accounting auth-web default
aaa accounting dot1x
aaa accounting login
aaa authentication auth-mac
aaa authentication auth-web
aaa authentication dot1x
aaa authentication login
radius-server host
server (Server Group)
aaa local authentication attempts lockout-time

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

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

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

Mode
Global Configuration

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

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

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

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

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

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

Related Commands
aaa local authentication attempts max-fail
aaa local authentication attempts max-fail

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

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

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

**Mode**
Global Configuration

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

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

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

**Examples**
To configure the number of login failures that will lock out a user account to two login attempts, use the commands:
```
awplus# configure terminal
awplus(config)# aaa local authentication attempts max-fail 2
```

To restore the number of login failures that will lock out a user account to the default number of login attempts (five login attempts), use the commands:
```
awplus# configure terminal
awplus(config)# no aaa local authentication attempts max-fail
```

**Related Commands**
- `aaa local authentication attempts lockout-time`
- `clear aaa local user lockout`
accounting login

**Overview**  This command applies a login accounting method list to console or vty lines for user login. When login accounting is enabled using this command, logging events generate an accounting record to the accounting server.

The accounting method list must be configured first using this command. If an accounting method list is specified that has not been created by this command then accounting will be disabled on the specified lines.

The no variant of this command resets AAA (Authentication, Authorization, Accounting) Accounting applied to console or vty lines for local or remote login. default login accounting is applied after issuing the no accounting login command. Accounting is disabled with default.

**Syntax**

```
accounting login {default|<list-name>}
no accounting login
```

**Default**  By default login accounting is disabled in the default accounting server. No accounting will be performed until accounting is enabled using this command beforehand.

**Mode**  Line Configuration

**Examples**  To apply the accounting server USERS to all vty lines use the following commands:

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

**Related Commands**

- aaa accounting commands
- aaa accounting login

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Default accounting method list.</td>
</tr>
<tr>
<td>&lt;list-name&gt;</td>
<td>Named accounting method list.</td>
</tr>
</tbody>
</table>
AAA COMMANDS
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}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Clear lockout for the specified user.</td>
</tr>
<tr>
<td>&lt;username&gt;</td>
<td>Specifies the user account.</td>
</tr>
<tr>
<td>all</td>
<td>Clear lockout for all user accounts.</td>
</tr>
</tbody>
</table>

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>Accounting debugging.</td>
</tr>
<tr>
<td>all</td>
<td>All debugging options are enabled.</td>
</tr>
<tr>
<td>authentication</td>
<td>Authentication debugging.</td>
</tr>
<tr>
<td>authorization</td>
<td>Authorization debugging.</td>
</tr>
</tbody>
</table>

**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
AAA COMMANDS
LOGIN AUTHENTICATION

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
```

Default
The default login authentication method list, as specified by the `aaa authentication login` command, is used to authenticate user login. If this has not been specified, the default is to use the local user database.

Mode
Line Configuration

Examples
To reset user authentication configuration on all VTY lines, use the following commands:
```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)# no login authentication
```

Related Commands
`aaa authentication login`
`line`
**show aaa local user locked**

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

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

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

**Mode**  
User Exec and Privileged Exec

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

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

**Output**  
Figure 37-1: Example output from the `show aaa local user locked` command

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

**Related Commands**
- `aaa local authentication attempts lockout-time`
- `aaa local authentication attempts max-fail`
- `clear aaa local user lockout`
show debugging aaa

**Overview**  This command displays the current debugging status for AAA (Authentication, Authorization, Accounting).

**Syntax**  show debugging aaa

**Mode**  User Exec and Privileged Exec

**Example**  To display the current debugging status of AAA, use the command:

```
awplus# show debug aaa
```

**Output**  Figure 37-2:  Example output from the *show debug aaa* command

```
AAA debugging status:
 Authentication debugging is on
 Accounting debugging is off
```
**Overview**  This command applies the functionality of the `no debug aaa` command.
Introduction

Overview This chapter provides an alphabetical reference for commands used to configure the device to use RADIUS servers.

Command List

- “deadtime (RADIUS server group)” on page 1649
- “debug radius” on page 1650
- “ip radius source-interface” on page 1651
- “radius-server deadtime” on page 1652
- “radius-server host” on page 1653
- “radius-server key” on page 1656
- “radius-server retransmit” on page 1657
- “radius-server timeout” on page 1659
- “server (Server Group)” on page 1661
- “show debugging radius” on page 1663
- “show radius” on page 1664
- “show radius statistics” on page 1666
- “undebug radius” on page 1667
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
```

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packet</td>
<td>Debugging for RADIUS packets is enabled or disabled.</td>
</tr>
<tr>
<td>event</td>
<td>Debugging for RADIUS events is enabled or disabled.</td>
</tr>
<tr>
<td>all</td>
<td>Enable or disable all debugging options.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>Interface name.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>IP address in the dotted decimal format A.B.C.D.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;minutes&gt;</td>
<td>RADIUS server deadtime in minutes in the range 0 to 1440 (24 hours).</td>
</tr>
</tbody>
</table>

**Default**
The default RADIUS deadtime configured on the system is 0 seconds.

**Mode**
Global Configuration

**Usage**
The RADIUS client considers a RADIUS server to be dead if it fails to respond to a request after it has been retransmitted as often as specified globally by the radius-server retransmit command or for the server by the radius-server host command. To improve RADIUS response times when some servers may be unavailable, set a **deadtime** to skip dead servers.

**Examples**
To set the dead time of the RADIUS server to 60 minutes, use the following commands:
```
awplus# configure terminal
awplus(config)# radius-server deadtime 60
```

To disable the dead time of the RADIUS server, use the following commands:
```
awplus# configure terminal
awplus(config)# no radius-server deadtime
```

**Related Commands**
deadtime (RADIUS server group)
radius-server host
radius-server retransmit
show radius statistics
radius-server host

**Overview**

Use this command to specify a remote RADIUS server host for authentication or accounting, and to set server-specific parameters. The parameters specified with this command override the corresponding global parameters for RADIUS servers. This command specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination UDP port numbers.

This command adds the RADIUS server address and sets parameters to the RADIUS server. The RADIUS server is added to the running configuration after you issue this command. If parameters are not set using this command then common system settings are applied.

Use the `no` variant of this command to remove the specified server host as a RADIUS authentication and/or accounting server and set the destination port to the default RADIUS server port number (1812).

**Syntax**

```
radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>] [key <key-string>] [retransmit <0-100>] [timeout <1-1000>]
```

```
no radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;host-name&gt;</code></td>
<td>Server host name. The DNS name of the RADIUS server host.</td>
</tr>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>The IP address of the RADIUS server host.</td>
</tr>
<tr>
<td>acct-port</td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;0-65535&gt;</code></td>
<td>UDP port number (Accounting port number is set to 1813 by default)</td>
</tr>
<tr>
<td>auth-port</td>
<td>Authentication port. Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the host is not used for authentication. The default UDP port for authentication is 1812.</td>
</tr>
<tr>
<td><code>&lt;0-65535&gt;</code></td>
<td>UDP port number (Authentication port number is set to 1812 by default)</td>
</tr>
<tr>
<td>timeout</td>
<td>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 <code>radius-server timeout</code> command is used.</td>
</tr>
</tbody>
</table>
## RADIUS-SERVER HOST

**Parameter** | **Description**
--- | ---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `<1-1000>` | Time in seconds to wait for a server reply (timeout is set to 5 seconds by default)  
The time interval (in seconds) to wait for the RADIUS server to reply before retransmitting a request or considering the server dead. This setting overrides the global value set by the `radius-server timeout` command.  
If no timeout value is specified for this server, the global value is used. |
| `retransmit` | Specifies the number of retries before skip to the next server. If this parameter is not specified the global value configured by the `radius-server retransmit` command is used. |
| `<0-100>` | Maximum number of retries (maximum number of retries is set to 3 by default)  
The maximum number of times to resend a RADIUS request to the server, if it does not respond within the timeout interval, before considering it dead and skipping to the next RADIUS server. This setting overrides the global setting of the `radius-server retransmit` command.  
If no retransmit value is specified, the global value is used. |
| `key` | Set shared secret key with RADIUS servers  
`<key-string>` | Shared key string applied  
Specifies the shared secret authentication or encryption key for all RADIUS communications between this device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the string are used. If spaces are used in the string, do not enclose the string in quotation marks unless the quotation marks themselves are part of the key. This setting overrides the global setting of the `radius-server key` command. If no key value is specified, the global value is used. |

**Default**  
The RADIUS client address is not configured (null) by default. No RADIUS server is configured.

**Mode**  
Global Configuration

**Usage**  
Multiple `radius-server host` commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified. If no host-specific timeout, retransmit, or key values are specified, the global values apply to that host. If there are multiple RADIUS servers for this client, use this command multiple times—one to specify each server.

If you specify a host without specifying the auth port or the acct port, it will by default be configured for both authentication and accounting, using the default UDP ports. To set a host to be a RADIUS server for authentication requests only, set the `acct-port` parameter to 0; to set the host to be a RADIUS server for accounting requests only, set the auth-port parameter to 0.

A RADIUS server is identified by IP address, authentication port and accounting port. A single host can be configured multiple times with different authentication or accounting ports. All the RADIUS servers configured with this command are
included in the predefined RADIUS server group radius, which may be used by AAA authentication, authorization and accounting commands. The client transmits (and retransmits, according to the retransmit and timeout parameters) RADIUS authentication or accounting requests to the servers in the order you specify them, until it gets a response.

**Examples**

To add the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20
```

To set the secret key to allied on the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 key allied
```

To delete the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host 10.0.0.20
```

To configure rad1.company.com for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad1.company.com acct-port 0
```

To remove the RADIUS server rad1.company.com configured for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host rad1.company.com acct-port 0
```

To configure rad2.company.com for accounting only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad2.company.com auth-port 0
```

To configure 192.168.1.1 with authentication port 1000, accounting port 1001 and retransmit count 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 192.168.1.1 auth-port 1000 acct-port 1001 retransmit 5
```

**Related Commands**

- `aaa group server`
- `radius-server key`
- `radius-server retransmit`
- `radius-server timeout`
- `show radius statistics`
radius-server key

**Overview**  This command sets a global secret key for RADIUS authentication on the device. The shared secret text string is used for RADIUS authentication between the device and a RADIUS server.

Note that if no secret key is explicitly specified for a RADIUS server, the global secret key will be used for the shared secret for the server.

Use the `no` variant of this command to reset the secret key to the default (null).

**Syntax**  
```
radius-server key <key>
no radius-server key
```

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;retries&gt;</code></td>
<td>RADIUS server retries in the range <code>&lt;0-100&gt;</code>. 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 <code>radius-server host</code> command, this global value is used.</td>
</tr>
</tbody>
</table>

**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 1813.

Use the `no` variant of this command to remove a RADIUS server from the server group.

**Syntax**

```
server {<hostname>|<ip-address>} [auth-port <0-65535>] [acct-port <0-65535>]
no server {<hostname>|<ip-address>} [auth-port <0-65535>] [acct-port <0-65535>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;hostname&gt;</code></td>
<td>Server host name</td>
</tr>
</tbody>
</table>
| `<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) |
RADIUS COMMANDS
SERVER (SERVER GROUP)

**Default**
The default Authentication port number is 1812 and the default Accounting port number is 1813.

**Mode**
Server Group Configuration

**Usage**
The RADIUS server to be added must be configured by the `radius-server host` command. In order to add or remove a server, the `auth-port` and `acct-port` parameters in this command must be the same as the corresponding parameters in the `radius-server host` command.

**Examples**
To create a RADIUS server group RAD_AUTH1 for authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_AUTH1
awplus(config-sg)# server 192.168.1.1 acct-port 0
awplus(config-sg)# server 192.168.2.1 auth-port 1000 acct-port 0
```

To create a RADIUS server group RAD_ACCT1 for accounting, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_ACCT1
awplus(config-sg)# server 192.168.2.1 auth-port 0 acct-port 1001
awplus(config-sg)# server 192.168.3.1 auth-port 0
```

To remove server 192.168.3.1 from the existing server group GROUP1, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no server 192.168.3.1
```

**Related Commands**
- `aaa accounting auth-mac default`
- `aaa accounting auth-web default`
- `aaa accounting dot1x`
- `aaa accounting login`
- `aaa authentication auth-mac`
- `aaa authentication auth-web`
- `aaa authentication login`
- `aaa group server`
- `radius-server host`
show debugging radius

**Overview**  This command displays the current debugging status for the RADIUS servers.

**Syntax**  show debugging radius

**Mode**  User Exec and Privileged Exec

**Example**  To display the current debugging status of RADIUS servers, use the command:

```
awplus# show debugging radius
```

**Output**  Figure 38-1:  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 38-2: 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

<table>
<thead>
<tr>
<th>Server Name/ IP Address</th>
<th>Auth Port</th>
<th>Acct Port</th>
<th>Auth Status</th>
<th>Acct Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.10</td>
<td>1812</td>
<td>1813</td>
<td>Alive</td>
<td>Alive</td>
</tr>
<tr>
<td>192.168.1.11</td>
<td>1812</td>
<td>N/A</td>
<td>Alive</td>
<td>N/A</td>
</tr>
</tbody>
</table>
```

**Example**
See the sample output below showing RADIUS client status and RADIUS configuration:
```
awplus# show radius
```
Output: Figure 38-3: Example output from the `show radius` command showing RADIUS client status

<table>
<thead>
<tr>
<th>Output Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Interface</td>
<td>The interface name or IP address to be used for the source address of all outgoing RADIUS packets.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>A shared secret key to a radius server.</td>
</tr>
<tr>
<td>Timeout</td>
<td>A time interval in seconds.</td>
</tr>
<tr>
<td>Retransmit Count</td>
<td>The number of retry count if a RADIUS server does not respond.</td>
</tr>
<tr>
<td>Deadtime</td>
<td>A time interval in minutes to mark a RADIUS server as “dead”.</td>
</tr>
<tr>
<td>Interim-Update</td>
<td>A time interval in minutes to send Interim-Update Accounting report.</td>
</tr>
<tr>
<td>Group Deadtime</td>
<td>The deadtime configured for RADIUS servers within a server group.</td>
</tr>
<tr>
<td>Server Host</td>
<td>The RADIUS server hostname or IP address.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>The destination UDP port for RADIUS authentication requests.</td>
</tr>
<tr>
<td>Accounting Port</td>
<td>The destination UDP port for RADIUS accounting requests.</td>
</tr>
<tr>
<td>Auth Status</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Alive</td>
</tr>
<tr>
<td></td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>Dead</td>
</tr>
<tr>
<td></td>
<td>Unknown</td>
</tr>
<tr>
<td>Acct Status</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 38-4: 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
```
RADIUS COMMANDS
UNDEBUG RADIUS

**undebug radius**

**Overview**  This command applies the functionality of the `no debug radius` command.
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.
LOCAL RADIUS SERVER COMMANDS

Command List

• “attribute” on page 1670
• “authentication” on page 1673
• “clear radius local-server statistics” on page 1674
• “copy fdb-radius-users (to file)” on page 1675
• “copy local-radius-user-db (from file)” on page 1677
• “copy local-radius-user-db (to file)” on page 1678
• “crypto pki enroll local” on page 1679
• “crypto pki enroll local local-radius-all-users” on page 1680
• “crypto pki enroll local user” on page 1681
• “crypto pki export local pem” on page 1682
• “crypto pki export local pkcs12” on page 1683
• “crypto pki trustpoint local” on page 1684
• “debug crypto pki” on page 1685
• “domain-style” on page 1686
• “egress-vlan-id” on page 1687
• “egress-vlan-name” on page 1689
• “group” on page 1691
• “nas” on page 1692
• “radius-server local” on page 1693
• “server auth-port” on page 1694
• “server enable” on page 1695
• “show crypto pki certificates” on page 1696
• “show crypto pki certificates local-radius-all-users” on page 1698
• “show crypto pki certificates user” on page 1700
• “show crypto pki trustpoints” on page 1702
• “show radius local-server group” on page 1703
• “show radius local-server nas” on page 1704
• “show radius local-server statistics” on page 1705
• “show radius local-server user” on page 1707
• “user (RADIUS server)” on page 1709
• “vlan (RADIUS server)” on page 1711
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 help parameter the attribute command displays a list of standard and vendor specific valid RADIUS attributes that are supported by the local RADIUS server.

If an attribute name is specified with the help parameter, then the attribute command displays a list of predefined attribute names. Note that you can only use the defined RADIUS attribute names and not define your own.

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 [<attribute-name>|<attribute-id>] help
attribute {<attribute-name>|<attribute-id>} <value>
no attribute {<attribute-name>|<attribute-id>}
```

**Parameter**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;attribute-name&gt;</td>
</tr>
<tr>
<td>&lt;attribute-id&gt;</td>
</tr>
<tr>
<td>&lt;value&gt;</td>
</tr>
<tr>
<td>help</td>
</tr>
</tbody>
</table>

**Default**  By default, no attributes are configured.

**Mode**  RADIUS Server Group Configuration

**Usage**  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 help
```

will produce the same results as the command:

```
awplus(config-radsrv-group)# attribute 49 help
```
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
```

**Examples**

To check a list of all available defined RADIUS attribute names, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# attribute help
```

A list of Vendor-specific Attributes displays after the list of defined Standard Attributes.

To get help for valid RADIUS attribute values for the attribute `Service-Type`, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# attribute Service-Type help
```

This results in the following output:

```
Service-Type : integer (Integer number)

Pre-defined values :
  Administrative-User (6)
  Authenticate-Only (8)
  Authorize-Only (17)
  Callback-Administrative (11)
  Callback-Framed-User (4)
  Callback-Login-User (3)
  Callback-NAS-Prompt (9)
  Call-Check (10)
  Framed-User (2)
  Login-User (1)
  NAS-Prompt-User (7)
  Outbound-User (5)
```
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
```
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}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac</td>
<td>Enable MAC authentication method.</td>
</tr>
<tr>
<td>eapmd5</td>
<td>Enable EAP-MD5 authentication method.</td>
</tr>
<tr>
<td>eaptls</td>
<td>Enable EAP-TLS authentication method.</td>
</tr>
<tr>
<td>peap</td>
<td>Enable EAP-PEAP authentication method.</td>
</tr>
</tbody>
</table>

**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.

```plaintext
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.

```plaintext
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no authentication eapmd5
```

**Related Commands**

- server enable
- show radius local-server statistics
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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nas</td>
<td>Clear the NAS (Network Access Server) statistics on the device. For example, clearing statistics stored for NAS server invalid passwords.</td>
</tr>
<tr>
<td>server</td>
<td>Clear the Local RADIUS Server statistics on the device. For example, clearing Local RADIUS Servers statistics for all failed login attempts.</td>
</tr>
<tr>
<td>user</td>
<td>Clear the Local RADIUS Server user statistics. For example, clearing statistics stored for the number of successful user logins.</td>
</tr>
</tbody>
</table>

**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|flash|nvs|usb|debug|tftp|scp|fserver|<url>}
[interface <port>] [vlan <vid>] [group <name>]
[export-vlan [<radius-group-name>]]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-radius-user-db</td>
<td>Copy the local RADIUS server users created to the local RADIUS server.</td>
</tr>
<tr>
<td>flash</td>
<td>Copy the local RADIUS server users created to Flash memory.</td>
</tr>
<tr>
<td>nvs</td>
<td>Copy the local RADIUS server users created to NVS memory.</td>
</tr>
<tr>
<td>usb</td>
<td>Copy the local RADIUS server users created to USB storage device.</td>
</tr>
<tr>
<td>debug</td>
<td>Copy the local RADIUS server users created to debug.</td>
</tr>
<tr>
<td>tftp</td>
<td>Copy the local RADIUS server users created to the TFTP destination.</td>
</tr>
<tr>
<td>scp</td>
<td>Copy the local RADIUS server users created to the SCP destination.</td>
</tr>
<tr>
<td>fserver</td>
<td>Copy the local RADIUS server users created to the remote file server.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>Copy the local RADIUS server users created to the specified URL.</td>
</tr>
<tr>
<td>interface &lt;port&gt;</td>
<td>Copy only MAC addresses learned on a specified device port. Wildcards may be used when specifying an interface name. For example, when you specify interface port1.* then this command generates RADIUS server users for MAC addresses learned on stack 1.</td>
</tr>
<tr>
<td>vlan &lt;vid&gt;</td>
<td>Copy only MAC addresses learned on a specified VLAN.</td>
</tr>
<tr>
<td>group &lt;name&gt;</td>
<td>Assign a group name to the local RADIUS server users created.</td>
</tr>
<tr>
<td>export-vlan</td>
<td>Export VLAN ID assigned to exported FDB entry.</td>
</tr>
<tr>
<td>&lt;radius-group-name&gt;</td>
<td>Prefix for Radius group name storing VLAN ID</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Usage**
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
  {flash|nvs|usb|tftp|scp|<destination-url>}
```

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)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flash</td>
<td>Copy to flash memory.</td>
</tr>
<tr>
<td>nvs</td>
<td>Copy to NVS memory.</td>
</tr>
<tr>
<td>usb</td>
<td>Copy to USB storage device.</td>
</tr>
<tr>
<td>tftp</td>
<td>Copy to TFTP destination.</td>
</tr>
<tr>
<td>scp</td>
<td>Copy to SCP destination.</td>
</tr>
<tr>
<td>&lt;destination-url&gt;</td>
<td>URL of the Destination file.</td>
</tr>
</tbody>
</table>
**crypto pki enroll local**

**Overview**  Use this command to obtain a system certificate from the Local CA (Certificate Authority).

Use the `no` variant of this command to delete system certificates created by a Local CA (Certificate Authority).

**Syntax**  
```plaintext
crypto pki enroll local
no crypto pki enroll local
```

**Default**  The system certificate is not available until this command is issued.

**Mode**  Global Configuration

**Examples**  
The following command obtains the system certificate from the Local CA (Certificate Authority).
```
awplus# configure terminal
awplus(config)# crypto pki enroll local
```

The following command deletes the system certificate created by the Local CA (Certificate Authority).
```
awplus# configure terminal
awplus(config)# no crypto pki enroll local
```

**Related Commands**  
- `crypto pki trustpoint local`
- `group`
**crypto pki enroll local local-radius-all-users**

**Overview**
Use this command to create certificates for all users registered in the local RADIUS server. These certificates are created by the Local Certificate Authority (CA) on the device.

**Syntax**
crypto pki enroll local local-radius-all-users

**Default**
By default, there are no certificates for users in the local RADIUS server.

**Mode**
Global Configuration

**Example**
The following command obtains the local RADIUS server certificates for the user from the Local CA (Certificate Authority).

```
awplus# configure terminal
awplus(config)# crypto pki enroll local local-radius-all-users
```

**Related Commands**
crypto pki trustpoint local
show crypto pki certificates
crypto pki enroll local user

**Overview**  
Use this command to obtain a local user certificate from the Local CA (Certificate Authority).

Use the **no** variant of this command to delete user certificates created by the Local CA (Certificate Authority).

**Syntax**  
crypto pki enroll local user <user-name>

no crypto pki enroll local user <user-name>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;user-name&gt;</td>
<td>User name.</td>
</tr>
</tbody>
</table>

**Default**  
By default, there is no user certificate.

**Mode**  
Global Configuration

**Examples**  
The following command obtains Tom’s certificate from the Local CA (Certificate Authority):

awplus# configure terminal
awplus(config)# crypto pki enroll local user Tom

The following command deletes Tom’s certificates created by the Local CA (Certificate Authority):

awplus# configure terminal
awplus(config)# no crypto pki enroll local user Tom

**Related Commands**  
crypto pki trustpoint local
show crypto pki certificates
**crypto pki export local pem**

**Overview**
Use this command to export the certificate associated with the Local CA to a PEM format file.

**Syntax**
crypto pki export local pem url `<url>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;url&gt;</code></td>
<td>URL string.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Example**
The following command exports the Local CA certificate to a PEM format file.
```
awplus# configure terminal
awplus(config)# crypto pki export local pem url tftp://192.168.1.1/cacert.pem
```

**Related Commands**
crypto pki enroll local
crypto pki export local pkcs12

**Overview**
Use this command to export a specified certificate to a PKCS12 format file. This command cannot be used for exporting certificates for the local system.

**Syntax**
crypto pki export local pkcs12 <user-name> <destination-url>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;user-name&gt;</td>
<td>User name.</td>
</tr>
<tr>
<td>&lt;destination-url&gt;</td>
<td>Destination URL string.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Examples**
The following commands exports a certificate for a user named **client** to a PKCS12 format file.

```bash
awplus# configure terminal
awplus(config)# crypto pki export local pkcs12 client tftp://192.168.1.1/cacert.pem
```

To export Tom’s certificate to PKSC12 format file, use the commands:

```bash
awplus# configure terminal
awplus(config)# crypto pki export local pksc12 Tom tftp://192.168.1.1/tom.pfx
```

**Related Commands**
crypto pki enroll local
crypto pki trustpoint local

**Overview**  Use this command to declare the Local CA (Certificate Authority) as the trustpoint that the system uses. The ca-trustpoint configuration mode is available after this command is issued.

Use the **no** variant of this command to delete all information and certificates associated with Local CA as the trustpoint.

**Syntax**  
```
crypto pki trustpoint local
no crypto pki trustpoint local
```

**Default**  Local CA is not a trustpoint.

**Mode**  Global Configuration

**Examples**  Use the following commands to declare the Local CA as the trustpoint.

```
awplus# configure terminal
awplus(config)# crypto pki trustpoint local
```

Use the following commands to delete all information and certificates associated with the Local CA.

```
awplus# configure terminal
awplus(config)# no crypto pki trustpoint local
```

To create a client certificate for all users registered to the local RADIUS server, use the following commands:

```
awplus(config)# crypto pki trustpoint local
awplus(ca-trust-point)# exit
awplus(config)# crypto pki enroll local alternative
```

**Related Commands**  
- `crypto pki enroll local`
- `show crypto pki trustpoints`
debug crypto pki

**Overview**  Use this command to enable Public Key Infrastructure (PKI) debugging. When PKI debugging is enabled, the PKI module starts generating diagnostic messages to the system log.

Use the `no` variant of this command to disable Public Key Infrastructure (PKI) debugging. When PKI debugging is disabled, the PKI module stops generating diagnostic messages to the system log.

**Syntax**  
```
depend crypto pki
no debug crypto pki
```

**Default**  PKI debugging is disabled by default

**Mode**  Privileged Exec

**Examples**  
To enable the PKI debugging facility, use the command:
```
awplus# debug crypto pki
```

To disable the PKI debugging facility, use the command:
```
awplus# no debug crypto pki
```
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}
```

**Default**  This feature is disabled by default.

**Mode**  RADIUS Server Configuration

**Usage**  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`

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>suffix-atsign</td>
<td>Enable at sign &quot;@&quot; delimited suffix style, i.e. &quot;user@domain&quot;.</td>
</tr>
<tr>
<td>ntdomain</td>
<td>Enable NT domain style, i.e. &quot;domain\user&quot;.</td>
</tr>
</tbody>
</table>
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
**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vlan-name&gt;</td>
<td>The VLAN name to be configured as the Egress-VLAN-Name attribute.</td>
</tr>
<tr>
<td>tagged</td>
<td>Set frames on the VLAN as tagged. This sets the tag indication field to indicate that all frames on this VLAN are tagged.</td>
</tr>
<tr>
<td>untagged</td>
<td>Set all frames on the VLAN as untagged. This sets the tag indication field to indicate that all frames on this VLAN are untagged.</td>
</tr>
</tbody>
</table>

**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
**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>
```

**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>
nos nas <ip-address>
```

**Mode**  RADIUS Server Configuration

**Examples**  
The following commands add the NAS with an IP address of 192.168.1.2 to the list of clients that may send authentication requests to the local RADIUS server. Note the shared key that this NAS will use to establish its identity is NAS_PASSWORD.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# nas 192.168.1.2 key NAS_PASSWORD
```

The following commands remove the NAS with an IP address of 192.168.1.2 from the list of clients that are allowed to send authentication requests to the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no nas 192.168.1.2
```

**Related Commands**  
`show radius local-server nas`
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
```

**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 crypto pki certificates

Overview
Use this command to display certificate information for Local CA and Local System certificates.

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 crypto pki certificates [local-ca|local]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-ca</td>
<td>Local CA certificate.</td>
</tr>
<tr>
<td>local</td>
<td>Local system certificate.</td>
</tr>
</tbody>
</table>

Mode
User Exec and Privileged Exec

Examples
The following command displays Local CA (Certificate Authority) certificate information.

awplus# show crypto pki certificates local-ca

The following command displays Local System certificate information.

awplus# show crypto pki certificates local

The following command displays information for all Local CA and Local System certificates.

awplus# show crypto pki certificates
Output

Table 39-1: Example output from the **show crypto pki certificates** command showing Local System and Local CA certificates

```plaintext
awplus#show crypto pki certificates
Certificate: Local System
  Data:
    Version: 3 (0x2)
    Serial Number: 4 (0x4)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
    Validity
      Not Before: Oct  8 07:50:55 2009 GMT
      Not After : Oct  6 07:50:55 2019 GMT
    Subject: O=Allied-Telesis, CN=Tom

Certificate: Local CA
  Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
    Validity
    Subject: O=Allied-Telesis, CN=Tom
```

Table 39-2: Parameters in the output of the **show crypto pki certificates** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>Certificate name.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the certificate.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Algorithm used for the certificate signature.</td>
</tr>
<tr>
<td>Issuer</td>
<td>Subject of issuer creating the certificate.</td>
</tr>
<tr>
<td>Validity</td>
<td>Validity period.</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject of the certificate.</td>
</tr>
</tbody>
</table>

Related Commands

**crypto pki enroll local**
show crypto pki certificates
local-radius-all-users

**Overview**
Use this command to display certificate information for local RADIUS server users.

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 crypto pki certificates local-radius-all-users

**Mode**
User Exec and Privileged Exec

**Example**
The following command displays information of all local RADIUS server user certificates.

```
awplus# show crypto pki certificates local-radius-all-users
```

**Output**

Table 39-3: Example output from the `show crypto pki certificates local-radius-all-users` command

```
awplus#show crypto pki certificates local-radius-all-users
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2 (0x2)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
    Validity
      Not Before: Oct 8 07:50:55 2009 GMT
      Not After : Oct 6 07:50:55 2019 GMT
    Subject: O=Allied-Telesis, CN=Tom
```

Table 39-4: Parameters in the output of the `show crypto pki certificates local-radius-all-users` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>Certificate name.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the certificate.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Algorithm used for the certificate signature.</td>
</tr>
<tr>
<td>Issuer</td>
<td>Subject of issuer creating the certificate.</td>
</tr>
</tbody>
</table>
### Table 39-4: Parameters in the output of the `show crypto pki certificates local-radius-all-users` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validity</td>
<td>Validity period.</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject of the certificate.</td>
</tr>
</tbody>
</table>

**Related Commands**

crypto pki enroll local local-radius-all-users
show crypto pki certificates user

**Overview**  Use this command to display certificate information for a specified local RADIUS server user.  

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 crypto pki certificates user [<user-name>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;user-name&gt;</code></td>
<td>User name.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**  The following command displays Tom’s certificate information.

```
awplus# show crypto pki certificates user Tom
```

**Output**

Table 39-5: Example output from the `show crypto pki certificates user` command to show certificate information for user Tom

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2 (0x2)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
    Validity
      Not Before: Oct 8 07:50:55 2009 GMT
      Not After : Oct 6 07:50:55 2019 GMT
    Subject: O=Allied-Telesis, CN=Tom
```

Table 39-6: Parameters in the output of the `show crypto pki certificates user` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>Certificate name.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the certificate.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Algorithm used for the certificate signature.</td>
</tr>
</tbody>
</table>
Table 39-6: Parameters in the output of the `show crypto pki certificates user` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer</td>
<td>Subject of issuer creating the certificate.</td>
</tr>
<tr>
<td>Validity</td>
<td>Validity period.</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject of the certificate.</td>
</tr>
</tbody>
</table>

**Related Commands**

crypto pki enroll local user
show crypto pki trustpoints

**Overview**  Use this command to display trustpoint information.
For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show crypto pki trustpoints

**Mode**  User Exec and Privileged Exec

**Example**  The following command displays trustpoint information.

```
awplus# show crypto pki trustpoint
```

**Output**

Table 39-7: Example output from the `show crypto pki trustpoints` command

<table>
<thead>
<tr>
<th>Trustpoint local:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject Name:</td>
</tr>
<tr>
<td>CN = AlliedwarePlusCA</td>
</tr>
<tr>
<td>o = Allied-Telesis</td>
</tr>
<tr>
<td>Serial Number:0C</td>
</tr>
</tbody>
</table>

Table 39-8: Parameters in the output of the `show crypto pki trustpoints` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject Name</td>
<td>CA certificate subject.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Current serial number of CA.</td>
</tr>
</tbody>
</table>

**Related Commands**  crypto pki enroll local
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show radius local-server group [<user-group-name>]
```

**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 39-9: Example output from the `show radius local-server group` command

<table>
<thead>
<tr>
<th>Group-Name</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetworkOperators</td>
<td>ManagementNet</td>
</tr>
<tr>
<td>NormalUsers</td>
<td>CommonNet</td>
</tr>
</tbody>
</table>

Table 39-10: Parameters in the output of the `show radius local-server group` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group-Name</td>
<td>Group name.</td>
</tr>
<tr>
<td>Vlan</td>
<td>VLAN name assigned to the group.</td>
</tr>
</tbody>
</table>

**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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show radius local-server nas [\(<ip-address>\)]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>Specify NAS IP address for show output.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Example**  
The following command displays NAS information.

```
awplus# show radius local-server nas
```

**Output**

Table 39-11: Example output from the `show radius local-server nas` command

<table>
<thead>
<tr>
<th>NAS-Address</th>
<th>Shared-Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1</td>
<td>awplus-local-radius-server</td>
</tr>
</tbody>
</table>

Table 39-12: Parameters in the output of the `show radius local-server nas` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS-Address</td>
<td>IP address of NAS.</td>
</tr>
<tr>
<td>Shared-Key</td>
<td>Shared key used for RADIUS connection.</td>
</tr>
</tbody>
</table>

**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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show radius local-server statistics

**Mode**  User Exec and Privileged Exec

**Usage**  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 39-13: Example output from the show radius local-server statistics command

<table>
<thead>
<tr>
<th>Server status</th>
<th>Successes</th>
<th>Failed Logins</th>
<th>Unknown NAS</th>
<th>Unknown EAP message</th>
<th>Unknown EAP auth type</th>
<th>Corrupted packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run (administrative status is enable)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Enabled methods: MAC EAP-MD5 EAP-TLS EAP-PEAP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAS: 127.0.0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Successes:0 Shared key mismatch:0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAS: 192.168.1.61</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Successes:0 Shared key mismatch:0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAS: 192.168.1.63</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Successes:1 Shared key mismatch:0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAS: 192.168.1.65</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Successes:0 Shared key mismatch:0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>Successes</td>
<td>Failures</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 “Controlling “show” Command Output” in 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
```

**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 39-14:** Example output from the **show radius local-server user** command

<table>
<thead>
<tr>
<th>User-Name</th>
<th>Password</th>
<th>Group</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tom</td>
<td>abcd</td>
<td>NetworkOperators</td>
<td>ManagementNet</td>
</tr>
</tbody>
</table>

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.

```
awplus# show radius local-server user Tom format csv
```

**Table 39-15:** Example output from the **show radius local-server user csv** command

```
true,"NetworkOperators","Tom","abcd",0,2099/01/01,"","","ManagementNet",false,3600,false,0,"",false
```
Table 39-16: Parameters in the output from the `show radius local-server user` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name</td>
<td>User name.</td>
</tr>
<tr>
<td>Password</td>
<td>User password.</td>
</tr>
<tr>
<td>Group</td>
<td>Group name assigned to the user.</td>
</tr>
<tr>
<td>Vlan</td>
<td>VLAN name assigned to the user.</td>
</tr>
</tbody>
</table>

**Related Commands**

- group
- user (RADIUS server)
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**
- `<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**
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 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
```plaintext
vlan {<vid>|<vlan-name>}
no vlan
```

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
```
40  

TACACS+  
Commands

Introduction

Overview  This chapter provides an alphabetical reference for commands used to configure the device to use TACACS+ servers. For more information about TACACS+, see the TACACS+ Feature Overview and Configuration Guide.

Command List  
- “show tacacs+” on page 1712  
- “tacacs-server host” on page 1713  
- “tacacs-server key” on page 1715  
- “tacacs-server timeout” on page 1716
show tacacs+

**Overview**  This command displays the current TACACS+ server configuration and status.

**Syntax**  `show tacacs+

**Mode**  User Exec and Privileged Exec

**Example**  To display the current status of TACACS+ servers, use the command:

```
awplus# show tacacs+
```

**Output**  Figure 40-1:  Example output from the `show tacacs+` command

<table>
<thead>
<tr>
<th>TACACS+ Global Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server Host/IP Address</th>
<th>Server</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.10</td>
<td>Alive</td>
<td></td>
</tr>
<tr>
<td>192.168.1.11</td>
<td>Unknown</td>
<td></td>
</tr>
</tbody>
</table>

Table 40-1:  Parameters in the output of the `show tacacs+` command

<table>
<thead>
<tr>
<th>Output Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>A time interval in seconds.</td>
</tr>
<tr>
<td>Server Host/IP Address</td>
<td>TACACS+ server hostname or IP address.</td>
</tr>
<tr>
<td>Server Status</td>
<td>The status of the authentication port.</td>
</tr>
<tr>
<td>Alive</td>
<td>The server is alive.</td>
</tr>
<tr>
<td>Dead</td>
<td>The server has timed out.</td>
</tr>
<tr>
<td>Error</td>
<td>The server is not responding or there is an error in the key string entered.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The server is never used or the status is unknown.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>The server is unreachable.</td>
</tr>
<tr>
<td>Unresolved</td>
<td>The server name can not be resolved.</td>
</tr>
</tbody>
</table>
**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>}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;host-name&gt;</code></td>
<td>Server host name. The DNS name of the TACACS+ server host.</td>
</tr>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>The IP address of the TACACS+ server host, in dotted decimal notation A.B.C.D.</td>
</tr>
<tr>
<td><code>key</code></td>
<td>Set shared secret key with TACACS+ servers.</td>
</tr>
<tr>
<td><code>8</code></td>
<td>Specifies that you are entering a password as a string that has already been encrypted instead of entering a plain text password. The running config displays the new password as an encrypted string even if password encryption is turned off.</td>
</tr>
<tr>
<td><code>&lt;key-string&gt;</code></td>
<td>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 <code>tacacs-server key</code> command. If no key value is specified, the global value is used.</td>
</tr>
</tbody>
</table>

**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:

```bash
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:

```bash
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:

```bash
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+ Commands

TACACS-SERVER KEY

**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

**Mode**
Global Configuration

**Usage**
Use this command to set the global secret key shared between this client and its TACACS+ servers. If no secret key is specified for a particular TACACS+ server using the `tacacs-server host` command, this global key is used.

**Examples**
To set the global secret key to `secret` for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server key secret
```

To delete the global secret key for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server key
```

**Related Commands**
tacacs-server host

show tacacs+

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;key-string&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;seconds&gt;</code></td>
<td>TACACS+ server timeout in seconds, in the range 1 to 1000.</td>
</tr>
</tbody>
</table>

**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+`
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.
SECURE SHELL (SSH) COMMANDS

Command List

- “banner login (SSH)” on page 1719
- “clear ssh” on page 1720
- “crypto key destroy hostkey” on page 1721
- “crypto key destroy userkey” on page 1722
- “crypto key generate hostkey” on page 1723
- “crypto key generate userkey” on page 1724
- “crypto key pubkey-chain knownhosts” on page 1725
- “crypto key pubkey-chain userkey” on page 1727
- “debug ssh client” on page 1729
- “debug ssh server” on page 1730
- “service ssh” on page 1731
- “show banner login” on page 1733
- “show crypto key hostkey” on page 1734
- “show crypto key pubkey-chain knownhosts” on page 1735
- “show crypto key pubkey-chain userkey” on page 1736
- “show crypto key userkey” on page 1737
- “show running-config ssh” on page 1738
- “show ssh” on page 1740
- “show ssh client” on page 1742
- “show ssh server” on page 1743
- “show ssh server allow-users” on page 1745
- “show ssh server deny-users” on page 1746
- “ssh” on page 1747
- “ssh client” on page 1749
- “ssh server” on page 1751
- “ssh server allow-users” on page 1753
- “ssh server authentication” on page 1755
- “ssh server deny-users” on page 1757
- “ssh server resolve-host” on page 1759
- “ssh server scp” on page 1760
- “ssh server sftp” on page 1761
- “undebug ssh client” on page 1762
- “undebug ssh server” on page 1763
SECURE SHELL (SSH) COMMANDS
BANNER LOGIN (SSH)

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}

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Specify a session ID in the range 1 to 65535 to delete a specific session.</td>
</tr>
<tr>
<td>all</td>
<td>Delete all SSH sessions.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Examples**  
To stop the current SSH session 123, use the command:

```
awplus# clear ssh 123
```

To stop all SSH sessions active on the device, use the command:

```
awplus# clear ssh all
```

**Related Commands**  
service ssh  
ssh
**crypto key destroy hostkey**

**Overview**  This command deletes the existing public and private keys of the SSH server. Note that for an SSH server to operate it needs at least one set of hostkeys configured before an SSH server is started.

**Syntax**  `crypto key destroy hostkey {dsa|rsa|rsal}

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsa</td>
<td>Deletes the existing DSA public and private keys.</td>
</tr>
<tr>
<td>rsa</td>
<td>Deletes the existing RSA public and private keys configured for SSH version 2 connections.</td>
</tr>
<tr>
<td>rsal</td>
<td>Deletes the existing RSA public and private keys configured for SSH version 1 connections.</td>
</tr>
</tbody>
</table>

**Mode**  Global Configuration

**Example**  To destroy the RSA host key used for SSH version 2 connections, use the commands:

```bash
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}
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;username&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>dsa</code></td>
<td>Deletes the existing DSA userkey.</td>
</tr>
<tr>
<td><code>rsa</code></td>
<td>Deletes the existing RSA userkey configured for SSH version 2 connections.</td>
</tr>
<tr>
<td><code>rsa1</code></td>
<td>Deletes the existing RSA userkey for SSH version 1 connections.</td>
</tr>
</tbody>
</table>

**Mode**  Global Configuration

**Example**  To destroy the RSA user key for the SSH user `remoteuser`, use the commands:
```
awplus# configure terminal
awplus(config)# crypto key destroy userkey remoteuser rsa
```

**Related Commands**
- `crypto key generate hostkey`
- `show ssh`
- `show crypto key hostkey`
**crypto key generate hostkey**

**Overview**  
This command generates public and private keys for the SSH server using either an RSA or DSA cryptography algorithm. You must define a host key before enabling the SSH server. Start SSH server using the `service ssh` command. If a host key exists with the same cryptography algorithm, this command replaces the old host key with the new key.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

**Syntax**  
`crypto key generate hostkey {dsa|rsa|rsa1} [<768-32768>]`

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsa</td>
<td>Creates a DSA hostkey. Both SSH version 1 and 2 connections can use the DSA hostkey.</td>
</tr>
<tr>
<td>rsa</td>
<td>Creates an RSA hostkey for SSH version 2 connections.</td>
</tr>
<tr>
<td>rsa1</td>
<td>Creates an RSA hostkey for SSH version 1 connections.</td>
</tr>
<tr>
<td>&lt;768-32768&gt;</td>
<td>The length in bits of the generated key. The default is 1024 bits.</td>
</tr>
</tbody>
</table>

**Default**  
1024 bits is the default key length. The DSA algorithm supports 1024 bits.

**Mode**  
Global Configuration

**Examples**  
To generate an RSA host key for SSH version 2 connections that is 2048 bits in length, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa 2048
```

To generate a DSA host key, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate dsa
```

**Related Commands**  
- `crypto key destroy hostkey`
- `service ssh`
- `show crypto key hostkey`
**crypto key generate userkey**

**Overview**
This command generates public and private keys for an SSH user using either an RSA or DSA cryptography algorithm. To use public key authentication, copy the public key of the user onto the remote SSH server.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

**Syntax**
crypto key generate userkey <username> {dsa|rsa|rsa1} [<768-32768>]

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;username&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>dsa</td>
<td>Creates a DSA userkey. Both SSH version 1 and 2 connections can use a key created with this command.</td>
</tr>
<tr>
<td>rsa</td>
<td>Creates an RSA userkey for SSH version 2 connections.</td>
</tr>
<tr>
<td>rsa1</td>
<td>Creates an RSA userkey for SSH version 1 connections.</td>
</tr>
<tr>
<td>&lt;768-32768&gt;</td>
<td>The length in bits of the generated key. The DSA algorithm supports only 1024 bits. Default: 1024.</td>
</tr>
</tbody>
</table>

**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 destroy 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|rsal]
```

```
no crypto key pubkey-chain knownhosts <1-65535>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Keyword used prior to specifying an IPv4 address</td>
</tr>
<tr>
<td>ipv6</td>
<td>Keyword used prior to specifying an IPv6 address</td>
</tr>
<tr>
<td>&lt;hostname&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>rsa</td>
<td>Specify the RSA public key of the server to be added to the known host database.</td>
</tr>
<tr>
<td>dsa</td>
<td>Specify the DSA public key of the server to be added to the known host database.</td>
</tr>
<tr>
<td>rsal</td>
<td>Specify the SSHv1 public key of the server to be added to the known host database.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Specify a key identifier when removing a key using the <strong>no</strong> parameter.</td>
</tr>
</tbody>
</table>

**Default**  If no cryptography algorithm is specified, then **rsa** is used as the default cryptography algorithm.

**Mode**  Privilege Exec

**Usage**  This command adds a public key of the specified SSH server to the known host database on the device. The key is retrieved from the server. The remote SSH server is verified by using this public key. The user is requested to check the key is correct before adding it to the database.

If the remote server’s host key is changed, or if the device does not have the public key of the remote server, then SSH clients will inform the user that the public key of the server is altered or unknown.
**Examples**

To add the RSA host key of the remote SSH host IPv4 address 192.0.2.11 to the known host database, use the command:

```
awplus# crypto key pubkey-chain knownhosts 192.0.2.11
```

To delete the second entry in the known host database, use the command:

```
awplus# no crypto key pubkey-chain knownhosts 2
```

**Validation Commands**

```
show crypto key pubkey-chain knownhosts
```
crypto key pubkey-chain userkey

**Overview**
This command adds a public key for an SSH user on the SSH server. This allows the SSH server to support public key authentication for the SSH user. When configured, the SSH user can access the SSH server without providing a password from the remote host.

The `no` variant of this command removes a public key for the specified SSH user that has been added to the public key chain. When a SSH user’s public key is removed, the SSH user can no longer login using public key authentication.

**Syntax**
crypto key pubkey-chain userkey <username> [filename]
no crypto key pubkey-chain userkey <username> <1-65535>

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;username&gt;</td>
<td>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</td>
</tr>
<tr>
<td>&lt;filename&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>The key ID number of the user’s key. Specify the key ID to delete a key.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Usage**
You should import the public key file from the client node. The device can read the data from a file on the flash or user terminal.

Or you can add a key as text into the terminal. To add a key as text into the terminal, first enter the command `crypto key pubkey-chain userkey <username>`, and hit [Enter]. Enter the key as text. Note that the key you enter as text must be a valid SSH RSA key, not random ASCII text. Use [Ctrl]+D after entering it to save the text and re-enter the normal command line mode.

Note you can generate a valid SSH RSA key on the device first using the `crypto key generate host rsa` command. View the SSH RSA key generated on the device using the `show crypto key 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
rsaAAAAB3NzaC1yc2EAAAABIBiwAAAIEAr1s7SokW5aw2fcOw1TStpb9J20bWluh...
To add a public key for the user graydon from the file key.pub, use the commands:

```plaintext
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:

```plaintext
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:

```plaintext
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**
depth ssh client [brief|full]
no debug ssh client

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>brief</td>
<td>Enables brief debug mode.</td>
</tr>
<tr>
<td>full</td>
<td>Enables full debug mode.</td>
</tr>
</tbody>
</table>

**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**
depth 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**  
depth ssh server [brief|full]
no debug ssh server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>brief</td>
<td>Enables brief debug mode.</td>
</tr>
<tr>
<td>full</td>
<td>Enables full debug mode.</td>
</tr>
</tbody>
</table>

**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**  
depth ssh client
show ssh server
undebug ssh server
### service ssh

**Overview**  
This command enables the Secure Shell server on the device. Once enabled, connections coming from SSH clients are accepted.

SSH server needs a host key before it starts. If an SSHv2 host key does not exist, then this command fails. If SSHv1 is enabled but a host key for SSHv1 does not exist, then SSH service is unavailable for version 1.

The **no** variant of this command disables the Secure Shell server. When the Secure Shell server is disabled, connections from SSH, SCP, and SFTP clients are not accepted. This command does not affect existing SSH sessions. To terminate existing sessions, use the **clear ssh** command.

**Syntax**

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

**Default**  
The Secure Shell server is disabled by default. Both IPv4 and IPv6 Secure Shell server are enabled when you issue **service ssh** without specifying the optional **ip** or **ipv6** parameters.

**Mode**  
Global Configuration

**Examples**

To enable both the IPv4 and the IPv6 Secure Shell server, use the commands:

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

To enable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ip
```

To enable the IPv6 Secure Shell server only, use the commands:

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

To disable both the IPv4 and the IPv6 Secure Shell server, use the commands:

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

To disable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ip
```

To disable the IPv6 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ipv6
```
Related Commands

crypto key generate hostkey
show running-config ssh
show ssh server
ssh server allow-users
ssh server deny-users
show banner login

**Overview**  This command displays the banner message configured on the device. The banner message is displayed to the remote user before user authentication starts.

**Syntax**  show banner login

**Mode**  User Exec, Privileged Exec, Global Configuration, Interface Configuration, Line Configuration

**Example**  To display the current login banner message, use the command:

```
awplus# show banner login
```

**Related Commands**  banner login (SSH)
show crypto key hostkey

Overview  This command displays the SSH host keys generated by RSA and DSA algorithm. A host key pair (public and private keys) is needed to enable SSH server. The private key remains on the device secretly. The public key is copied to SSH clients to identify the server.

Syntax  show crypto key hostkey [dsa|rsa|rsa1]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsa</td>
<td>Displays the DSA algorithm public key.</td>
</tr>
<tr>
<td>rsa</td>
<td>Displays the RSA algorithm public key for SSH version 2 connections.</td>
</tr>
<tr>
<td>rsa1</td>
<td>Displays the RSA algorithm public key for SSH version 1 connections.</td>
</tr>
</tbody>
</table>

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 41-1: Example output from the show crypto key hostkey command

<table>
<thead>
<tr>
<th>Type</th>
<th>Bits</th>
<th>Fingerprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsa1</td>
<td>1024</td>
<td>e2:1c:c8:8b:d8:6e:19:c8:f4:ec:00:a2:71:4e:85:8b</td>
</tr>
</tbody>
</table>

Table 41-1: Parameters in output of the show crypto key hostkey command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Algorithm used to generate the key.</td>
</tr>
<tr>
<td>Bits</td>
<td>Length in bits of the key.</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Checksum value for the public key.</td>
</tr>
</tbody>
</table>

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]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65535&gt;</td>
<td>Key identifier for a specific key. Displays the public key of the entry if specified.</td>
</tr>
</tbody>
</table>

**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 41-2: Example output from the `show crypto key public-chain knownhosts` command

<table>
<thead>
<tr>
<th>No</th>
<th>Hostname</th>
<th>Type</th>
<th>Fingerprint</th>
</tr>
</thead>
</table>

Table 41-2: Parameters in the output of the `show crypto key public-chain knownhosts` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Number ID of the key.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Host name of the known SSH server.</td>
</tr>
<tr>
<td>Type</td>
<td>The algorithm used to generate the key.</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Checksum value for the public key.</td>
</tr>
</tbody>
</table>

**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**
- `<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 41-3: Example output from the `show crypto key public-chain userkey` command
```
No Type Bits Fingerprint
---------------------------------------------
```

Table 41-3: Parameters in the output of the `show crypto key userkey` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Number ID of the key.</td>
</tr>
<tr>
<td>Type</td>
<td>The algorithm used to generate the key.</td>
</tr>
<tr>
<td>Bits</td>
<td>Length in bits of the key.</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Checksum value for the key.</td>
</tr>
</tbody>
</table>

**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**
- `<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 41-4: Example output from the show crypto key userkey command

<table>
<thead>
<tr>
<th>Type</th>
<th>Bits</th>
<th>Fingerprint</th>
</tr>
</thead>
</table>

Table 41-4: Parameters in the output of the `show crypto key userkey` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The algorithm used to generate the key.</td>
</tr>
<tr>
<td>Bits</td>
<td>Length in bits of the key.</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Checksum value for the key.</td>
</tr>
</tbody>
</table>

**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 41-5: 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 41-5: Parameters in the output of the show running-config ssh command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh server</td>
<td>SSH server is enabled.</td>
</tr>
<tr>
<td>ssh server v2</td>
<td>SSH server is enabled and only support SSHv2.</td>
</tr>
<tr>
<td>ssh server&lt;port&gt;</td>
<td>SSH server is enabled and listening on the specified TCP port.</td>
</tr>
<tr>
<td>no ssh server scp</td>
<td>SCP service is disabled.</td>
</tr>
<tr>
<td>no ssh server sftp</td>
<td>SFTP service is disabled.</td>
</tr>
<tr>
<td>ssh server session-timeout</td>
<td>Configure the server session timeout.</td>
</tr>
<tr>
<td>ssh server login-timeout</td>
<td>Configure the server login timeout.</td>
</tr>
<tr>
<td>ssh server max-startups</td>
<td>Configure the maximum number of concurrent sessions waiting authentication.</td>
</tr>
<tr>
<td>no ssh server authentication password</td>
<td>Password authentication is disabled.</td>
</tr>
<tr>
<td>no ssh server authentication publickey</td>
<td>Public key authentication is disabled.</td>
</tr>
</tbody>
</table>
Table 41-5: Parameters in the output of the **show running-config ssh** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh server allow-users</td>
<td>Add the user (and hostname) to the allow list.</td>
</tr>
<tr>
<td>ssh server deny-users</td>
<td>Add the user (and hostname) to the deny list.</td>
</tr>
</tbody>
</table>

**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 41-6: Example output from the show ssh command

<table>
<thead>
<tr>
<th>Secure Shell Sessions:</th>
<th>ID</th>
<th>Type</th>
<th>Peer Host</th>
<th>Username</th>
<th>State</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>414</td>
<td>ssh</td>
<td>172.16.23.1</td>
<td>root</td>
<td>open</td>
<td></td>
</tr>
<tr>
<td></td>
<td>456</td>
<td>ssh</td>
<td>172.16.23.10</td>
<td>manager</td>
<td>user-auth</td>
<td></td>
</tr>
<tr>
<td></td>
<td>459</td>
<td>scp</td>
<td>172.16.23.12</td>
<td>root</td>
<td>download</td>
<td>550dev_.awd</td>
</tr>
<tr>
<td></td>
<td>463</td>
<td>ssh</td>
<td>5ffe:33fe:5632:ffbb:bc35:dede:0101:ac51</td>
<td>manager</td>
<td>user-auth</td>
<td></td>
</tr>
</tbody>
</table>

Table 41-6: Parameters in the output of the show ssh command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Unique identifier for each SSH session.</td>
</tr>
<tr>
<td>Type</td>
<td>Session type; either SSH, SCP, or SFTP.</td>
</tr>
<tr>
<td>Mode</td>
<td>Whether the device is acting as an SSH client (client) or SSH server (server) for the specified session.</td>
</tr>
<tr>
<td>Peer Host</td>
<td>The hostname or IP address of the remote server or client.</td>
</tr>
<tr>
<td>Username</td>
<td>Login user name of the server.</td>
</tr>
</tbody>
</table>
### Table 41-6: Parameters in the output of the `show ssh` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>The current state of the SSH session. One of:</td>
</tr>
<tr>
<td>connecting</td>
<td>The device is looking for a remote server.</td>
</tr>
<tr>
<td>connected</td>
<td>The device is connected to the remote server.</td>
</tr>
<tr>
<td>accepted</td>
<td>The device has accepted a new session.</td>
</tr>
<tr>
<td>host-auth</td>
<td>Host-to-host authentication is in progress.</td>
</tr>
<tr>
<td>user-auth</td>
<td>User authentication is in progress.</td>
</tr>
<tr>
<td>authenticated</td>
<td>User authentication is complete.</td>
</tr>
<tr>
<td>open</td>
<td>The session is in progress.</td>
</tr>
<tr>
<td>download</td>
<td>The user is downloading a file from the device.</td>
</tr>
<tr>
<td>upload</td>
<td>The user is uploading a file from the device.</td>
</tr>
<tr>
<td>closing</td>
<td>The user is terminating the session.</td>
</tr>
<tr>
<td>closed</td>
<td>The session is closed.</td>
</tr>
<tr>
<td><strong>Filename</strong></td>
<td>Local filename of the file that the user is downloading or uploading.</td>
</tr>
</tbody>
</table>

**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 41-7:  Example output from the **show ssh client** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>SSH server TCP port where the SSH client connects to. The default is port 22.</td>
</tr>
<tr>
<td>Version</td>
<td>SSH server version; either &quot;1&quot;, &quot;2&quot; or &quot;2,1&quot;.</td>
</tr>
<tr>
<td>Connect Timeout</td>
<td>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.</td>
</tr>
<tr>
<td>Debug</td>
<td>Whether debugging is active on the client.</td>
</tr>
</tbody>
</table>

Table 41-7: Parameters in the output of the **show ssh client** command

**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 41-8:  Example output from the `show ssh server` command

<table>
<thead>
<tr>
<th>Secure Shell Server Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Server</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Version</td>
</tr>
<tr>
<td>Services</td>
</tr>
<tr>
<td>User Authentication</td>
</tr>
<tr>
<td>Idle Timeout</td>
</tr>
<tr>
<td>Maximum Startups</td>
</tr>
<tr>
<td>Debug</td>
</tr>
</tbody>
</table>

Table 41-8:  Parameters in the output of the `show ssh server` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Server</td>
<td>Whether the Secure Shell server is enabled or disabled.</td>
</tr>
<tr>
<td>Port</td>
<td>TCP port where the Secure Shell server listens for connections. The default is port 22.</td>
</tr>
<tr>
<td>Version</td>
<td>SSH server version; either “1”, “2” or “2,1”.</td>
</tr>
<tr>
<td>Services</td>
<td>List of the available Secure Shell service; one or more of SHELL, SCP or SFTP.</td>
</tr>
<tr>
<td>Authentication</td>
<td>List of available authentication methods.</td>
</tr>
<tr>
<td>Login Timeout</td>
<td>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.</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>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.</td>
</tr>
</tbody>
</table>
SECURE SHELL (SSH) COMMANDS
SHOW SSH SERVER

Table 41-8: Parameters in the output of the **show ssh server** command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Startups</td>
<td>The maximum number of concurrent connections that are waiting authentication. The default is 10.</td>
</tr>
<tr>
<td>Debug</td>
<td>Whether debugging is active on the server.</td>
</tr>
</tbody>
</table>

**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 41-9: Example output from the `show ssh server allow-users` command

<table>
<thead>
<tr>
<th>Username</th>
<th>Remote Hostname (pattern)</th>
</tr>
</thead>
<tbody>
<tr>
<td>awplus</td>
<td>192.168.*</td>
</tr>
<tr>
<td>john</td>
<td></td>
</tr>
<tr>
<td>manager</td>
<td><em>.</em>.alliedtelesis.com</td>
</tr>
</tbody>
</table>

Table 41-9: Parameters in the output of the `show ssh server allow-users` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>User name that is allowed to access the SSH server.</td>
</tr>
<tr>
<td>Remote Hostname (pattern)</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 41-10: Example output from the show ssh server deny-users command

<table>
<thead>
<tr>
<th>Username</th>
<th>Remote Hostname (pattern)</th>
</tr>
</thead>
<tbody>
<tr>
<td>john</td>
<td>*.b-company.com</td>
</tr>
<tr>
<td>manager</td>
<td>192.168.2.*</td>
</tr>
</tbody>
</table>

Table 41-10: Parameters in the output of the show ssh server deny-users command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The user that this rule applies to.</td>
</tr>
<tr>
<td>Remote Hostname (pattern)</td>
<td>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.</td>
</tr>
</tbody>
</table>

Related Commands

ssh server allow-users
ssh server deny-users
**ssh**

**Overview**  This command initiates a Secure Shell connection to a remote SSH server.

If the server requests a password for the user login, the user needs to type in the correct password on “Password:” prompt.

SSH client identifies the remote SSH server by its public key registered on the client device. If the server identification is changed, server verification fails. If the public key of the server has been changed, the public key of the server must be explicitly added to the known host database.

*NOTE: Note that any hostname specified with ssh cannot begin with a hyphen (-) character.*

**Syntax**  
```plaintext
ssh [ip|ipv6][[<user <username>]]|<port <1-65535>]|<version [1|2]))] <hostname> [<line>]
```

**Parameter** | **Description**
--- | ---
**ip** | Specify IPv4 SSH.
**ipv6** | Specify IPv6 SSH.
**user** | Login user. If user is specified, the username is used for login to the remote SSH server when user authentication is required. Otherwise the current user name is used.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User name to login on the remote server.</td>
</tr>
</tbody>
</table>

**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.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TCP port.</td>
</tr>
</tbody>
</table>

**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.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use SSH version 1.</td>
</tr>
<tr>
<td></td>
<td>Use SSH version 2.</td>
</tr>
</tbody>
</table>

**<hostname>** | IPv4/IPv6 address or hostname of a remote server in the format a.b.c.d for an IPv4 address, or in the format x:x:x:x for an IPv6 address corresponding to the ip or ipv6 optional keywords used. Note that any hostname specified with ssh cannot begin with a hyphen (-) character.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
**Mode**  User Exec and Privileged Exec

**Examples**  To login to the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 as user manager, use the command:

```
awplus# ssh ip user manager 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 that is listening TCP port 2000, use the command:

```
awplus# ssh port 2000 192.0.2.5
```

To login to the remote SSH server with example_host using IPv6 session, use the command:

```
awplus# ssh ipv6 example_host
```

To run the cmd command on the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5 cmd
```

**Related Commands**  
crypto key generate userkey
crypto key pubkey-chain knownhosts
debug ssh client

ssh client
**ssh client**

**Overview** This command modifies the default configuration parameters of the Secure Shell (SSH) client. The configuration is used for any SSH client on the device to connect to remote SSH servers. Any parameters specified on SSH client explicitly override the default configuration parameters.

The change affects the current user shell only. When the user exits the login session, the configuration does not persist. This command does not affect existing SSH sessions.

The **no** variant of this command resets configuration parameters of the Secure Shell (SSH) client changed by the `ssh client` command, and restores the defaults. This command does not affect the existing SSH sessions.

**Syntax**

```
ssh client {port <1-65535>|version {1|2}|session-timeout <0-3600>|connect-timeout <1-600>}
no ssh client {port|version|session-timeout|connect-timeout}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>port</strong></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>&lt;1-65535&gt; TCP port number.</td>
</tr>
<tr>
<td><strong>version</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>1 SSH clients on the device supports SSH version 1 only.</td>
</tr>
<tr>
<td></td>
<td>2 SSH clients on the device supports SSH version 2 only</td>
</tr>
<tr>
<td><strong>session-timeout</strong></td>
<td>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)</td>
</tr>
<tr>
<td></td>
<td>&lt;0-3600&gt; Timeout in seconds.</td>
</tr>
<tr>
<td><strong>connect-timeout</strong></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>&lt;1-600&gt; Timeout in seconds.</td>
</tr>
</tbody>
</table>
SECURE SHELL (SSH) COMMANDS

SSH CLIENT

<table>
<thead>
<tr>
<th>Mode</th>
<th>Privileged Exec</th>
</tr>
</thead>
</table>
| Examples      | To configure the default TCP port for SSH clients to 2200, and the session timer to 10 minutes, use the command:  
awplus# ssh client port 2200 session-timeout 600  
To configure the connect timeout of SSH client to 10 seconds, use the command:  
awplus# ssh client connect-timeout 10  
To restore the connect timeout to its default, use the command:  
awplus# no ssh client connect-timeout |
| Related Commands | show ssh client  
ssh |
ssh server

**Overview**  This command modifies the configuration of the SSH server. Changing these parameters affects new SSH sessions connecting to the device.

The `no` variant of this command restores the configuration of a specified parameter to its default. The change affects the SSH server immediately if the server is running. Otherwise, the configuration is used when the server starts.

To enable the SSH server, use the `service ssh` command.

**Syntax**

```plaintext
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]}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1v2</td>
<td>Supports both SSHv2 and SSHv1 client connections. Default: v1v2</td>
</tr>
<tr>
<td>v2only</td>
<td>Supports SSHv2 client connections only.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>The TCP port number that the server listens to for incoming SSH sessions. Default: 22</td>
</tr>
<tr>
<td>session-timeout</td>
<td>There is a maximum time period that the server waits before deciding that a session is inactive and should be terminated. The server considers the session inactive when it has not received any data from the client, and when the client does not respond to keep alive messages. Default: 0 (session timer remains off).</td>
</tr>
<tr>
<td>login-timeout</td>
<td>The maximum time period the server waits before disconnecting an unauthenticated client. Default: 60</td>
</tr>
<tr>
<td>max-startups</td>
<td>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</td>
</tr>
</tbody>
</table>

**Mode**  Global Configuration
**Examples**

To configure the session timer of SSH server to 10 minutes (600 seconds), use the commands:

```bash
awplus# configure terminal
awplus(config)# ssh server login-timeout 600
```

To configure the login timeout of SSH server to 30 seconds, use the commands:

```bash
awplus# configure terminal
awplus(config)# ssh server login-timeout 30
```

To limit the number of SSH client connections waiting authentication from SSH server to 3, use the commands:

```bash
awplus# configure terminal
awplus(config)# ssh server max-startups
```

To set max-startups parameters of SSH server to the default configuration, use the commands:

```bash
awplus# configure terminal
awplus(config)# no ssh server max-startups
```

To support the Secure Shell server with TCP port 2200, use the commands:

```bash
awplus# configure terminal
awplus(config)# ssh server 2200
```

To force the Secure Shell server to support SSHv2 only, use the commands:

```bash
awplus# configure terminal
awplus(config)# ssh server v2only
```

To support both SSHv2 and SSHv1, use the commands:

```bash
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>]
```

**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}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>Specifies user password authentication for SSH server.</td>
</tr>
<tr>
<td>publickey</td>
<td>Specifies user publickey authentication for SSH server.</td>
</tr>
</tbody>
</table>

**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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;username-pattern&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;hostname-pattern&gt;</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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`
Secure Shell (SSH) Commands
SSH Server Resolve-Host

**ssh server resolve-host**

**Overview**  This command enables resolving an IP address from a host name using a DNS server for client host authentication.

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

**Syntax**  
```
ssh server resolve-hosts
no ssh server resolve-hosts
```

**Default**  This feature is disabled by default.

**Mode**  Global Configuration

**Usage**  Your device has a DNS Client that is enabled automatically when you add a DNS server to your device. Use the **ip name-server** command to add a DNS server to the list of servers that the device queries.

For information about configuring DNS, see the Internet Protocol Feature Overview and Configuration Guide.

**Example**  To resolve a host name using a DNS server, use the commands:
```
awplus# configure terminal
awplus(config)# ssh server resolve-hosts
```

**Related Commands**  
- **ip name-server**
- **show ssh server**
- **ssh server allow-users**
- **ssh server deny-users**
ssh server scp

**Overview**
This command enables the Secure Copy (SCP) service on the SSH server. Once enabled, the server accepts SCP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SCP connections. The SCP service is enabled by default as soon as the SSH server is enabled.

The *no* variant of this command disables the SCP service on the SSH server. Once disabled, SCP requests from remote clients are rejected.

**Syntax**
- `ssh server scp`
- `no ssh server scp`

**Mode**
Global Configuration

**Examples**
To enable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server scp
```

To disable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server scp
```

**Related Commands**
- `show running-config ssh`
- `show ssh server`
**ssh server sftp**

**Overview**  
This command enables the Secure FTP (SFTP) service on the SSH server. Once enabled, the server accepts SFTP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SFTP connections. The SFTP service is enabled by default as soon as the SSH server is enabled. If the SSH server is disabled, SFTP service is unavailable.

The `no` variant of this command disables SFTP service on the SSH server. Once disabled, SFTP requests from remote clients are rejected.

**Syntax**  
```
ssh server sftp
no ssh server sftp
```

**Mode**  
Global Configuration

**Examples**  
To enable the SFTP service, use the commands:
```
awplus# configure terminal
awplus(config)# ssh server sftp
```

To disable the SFTP service, use the commands:
```
awplus# configure terminal
awplus(config)# no ssh server sftp
```

**Related Commands**  
`show running-config ssh`

`show ssh server`
**Overview**  This command applies the functionality of the *no debug ssh client* command.
**Overview**  
This command applies the functionality of the `no debug ssh server` command.
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).
DHCP SNOOPING COMMANDS

Command List

- “arp security” on page 1765
- “arp security violation” on page 1766
- “clear arp security statistics” on page 1768
- “clear ip dhcp snooping binding” on page 1769
- “clear ip dhcp snooping statistics” on page 1770
- “debug arp security” on page 1771
- “debug ip dhcp snooping” on page 1772
- “ip dhcp snooping” on page 1773
- “ip dhcp snooping agent-option” on page 1774
- “ip dhcp snooping agent-option allow-untrusted” on page 1775
- “ip dhcp snooping agent-option circuit-id vlantriplet” on page 1776
- “ip dhcp snooping agent-option remote-id” on page 1777
- “ip dhcp snooping binding” on page 1778
- “ip dhcp snooping database” on page 1779
- “ip dhcp snooping delete-by-client” on page 1780
- “ip dhcp snooping delete-by-linkdown” on page 1781
- “ip dhcp snooping max-bindings” on page 1782
- “ip dhcp snooping subscriber-id” on page 1783
- “ip dhcp snooping trust” on page 1784
- “ip dhcp snooping verify mac-address” on page 1785
- “ip dhcp snooping violation” on page 1786
- “ip source binding” on page 1787
- “service dhcp-snooping” on page 1789
- “show arp security” on page 1791
- “show arp security interface” on page 1792
- “show arp security statistics” on page 1794
- “show debugging arp security” on page 1796
- “show debugging ip dhcp snooping” on page 1797
- “show ip dhcp snooping” on page 1798
- “show ip dhcp snooping acl” on page 1799
- “show ip dhcp snooping agent-option” on page 1802
- “show ip dhcp snooping binding” on page 1803
- “show ip dhcp snooping interface” on page 1805
- “show ip dhcp snooping statistics” on page 1809
- “show ip source binding” on page 1812
arp security

**Overview**
Use this command to enable ARP security on untrusted ports in the VLANs, so that
the switch only responds to/forwards ARP packets if they have recognized IP and
MAC source addresses.

Use the no variant of this command to disable ARP security on the VLANs.

**Syntax**
arp security
no arp security

**Default** Disabled

**Mode** Interface Configuration (VLANS)

**Usage**
Enable ARP security to provide protection against ARP spoofing. DHCP snooping
must also be enabled on the switch (service dhcp-snooping command), and on the
VLANS (ip dhcp snooping command).

**Example**
To enable ARP security on VLANs 2 to 4, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# arp security
```

**Related Commands**
arp security violation
show arp security
show arp security interface
show arp security statistics
arp security violation

**Overview**
Use this command to specify an additional action to perform if an ARP security violation is detected on the ports. ARP security must also be enabled (arp security command).

Use the `no` variant of this command to remove the specified action, or all actions. Traffic violating ARP security will be dropped, but no other action will be taken.

**Syntax**
```
arp security violation {log|trap|link-down} ...
no arp security violation [log|trap|link-down] ...
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>Generate a log message. To display these messages, use the <code>show log</code> command.</td>
</tr>
<tr>
<td>trap</td>
<td>Generate an SNMP notification (trap). To send SNMP notifications, SNMP must also be configured, and DHCP snooping notifications must be enabled using the <code>snmp-server enable trap</code> 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.</td>
</tr>
<tr>
<td>link-down</td>
<td>Shut down the port that received the packet. Default: disabled.</td>
</tr>
</tbody>
</table>

**Default**
When the switch detects an ARP security violation, it drops the packet. By default, it does not perform any other violation actions.

**Mode**
Interface Configuration (switch ports, static or dynamic aggregated links)

**Usage**
When the switch detects an ARP security violation on an untrusted port in a VLAN that has ARP security enabled, it drops the packet. This command sets the switch to perform additional actions in response to ARP violations.

If a port has been shut down in response to a violation, to bring it back up again after any issues have been resolved, use the `shutdown` command.

**Example**
To send SNMP notifications for ARP security violations on ports 1.0.1 to 1.0.6, use the commands:
```
awplus# configure terminal
awplus(config)# snmp-server enable trap dhcpsnooping
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# arp security violation trap
```
DHCP SNOOPING COMMANDS
ARP SECURITY VIOLATION

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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(&lt;ipaddr&gt;)</td>
<td>Remove the entry for this client IP address.</td>
</tr>
<tr>
<td>(&lt;port-list&gt;)</td>
<td>Remove all entries for these ports. The port list may contain switch ports, and static or dynamic link aggregators (channel groups).</td>
</tr>
<tr>
<td>(&lt;vid-list&gt;)</td>
<td>Remove all entries associated with these VLANs.</td>
</tr>
</tbody>
</table>

**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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
To clear statistics for the DHCP snooping on interface port1.0.1, use the command:

```bash
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]}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All DHCP snooping debug.</td>
</tr>
<tr>
<td>acl</td>
<td>DHCP snooping access list debug.</td>
</tr>
<tr>
<td>db</td>
<td>DHCP snooping binding database debug.</td>
</tr>
<tr>
<td>packet</td>
<td>DHCP snooping packet debug. For the <code>no</code> variant of this command, this option also disables detailed packet debug, if it was enabled.</td>
</tr>
<tr>
<td>detail</td>
<td>Detailed packet debug.</td>
</tr>
</tbody>
</table>

**Default**  Disabled

**Mode**  Privileged Exec

**Example**  To enable access list debugging for DHCP snooping, use the commands:
```
awplus# debug ip dhcp snooping acl
```

**Related Commands**
- `debug arp security`
- `show debugging ip dhcp snooping`
- `show log`
- `terminal monitor`
**ip dhcp snooping**

**Overview**  Use this command to enable DHCP snooping on one or more VLANs. Use the no variant of this command to disable DHCP snooping on the VLANs.

**Syntax**  
```
ip dhcp snooping
no ip dhcp snooping
```

**Default**  DHCP snooping is disabled on VLANs by default.

**Mode**  Interface Configuration (VLANs)

**Usage**  For DHCP snooping to operate on a VLAN, it must:
- be enabled on the particular VLAN by using this command
- be enabled globally on the switch by using the `service dhcp-snooping` command
- have at least one port connected to a DHCP server configured as a trusted port by using the `ip dhcp snooping trust` command

Any ACLs on a port that permit traffic matching DHCP snooping entries and block other traffic, will block all traffic if DHCP snooping is disabled on the port. If you disable DHCP snooping on particular VLANs using this command, you must also remove any DHCP snooping ACLs from the ports to maintain connectivity (no `access-group` command).

**Examples**  To enable DHCP snooping on VLANs 2 to 4, use the commands:
```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ip dhcp snooping
```

To disable DHCP snooping on the switch, use the command:
```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no ip dhcp snooping
```

**Related Commands**  
- ip dhcp snooping trust
- service dhcp-snooping
- show ip dhcp snooping
**Overview**

Use this command to enable DHCP Relay Agent Option 82 information insertion on the switch. When this is enabled, the switch:

- inserts DHCP Relay Agent Option 82 information into DHCP packets that it receives on untrusted ports
- removes DHCP Relay Agent Option 82 information from DHCP packets that it sends to untrusted ports.

Use the `no` variant of this command to disable DHCP Relay Agent Option 82 insertion.

**Syntax**

```
ip dhcp snooping agent-option
no ip dhcp snooping agent-option
```

**Default**

DHCP Relay Agent Option 82 insertion is enabled by default when DHCP snooping is enabled.

**Mode**

Global Configuration

**Usage**

DHCP snooping must also be enabled on the switch (`service dhcp-snooping` command), and on the VLANs (`ip dhcp snooping` command).

If a subscriber ID is configured for the port (`ip dhcp snooping subscriber-id` command), the switch includes this in the DHCP Relay Agent Option 82 information it inserts into DHCP packets received on the port.

**Example**

To disable DHCP Relay Agent Option 82 on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping agent-option
```

**Related Commands**

- `ip dhcp snooping`
- `ip dhcp snooping agent-option allow-untrusted`
- `ip dhcp snooping subscriber-id`
- `service dhcp-snooping`
- `show ip dhcp snooping`
**ip dhcp snooping agent-option allow-untrusted**

**Overview**
Use this command to enable DHCP Relay Agent Option 82 information reception on untrusted ports. When this is enabled, the switch accepts incoming DHCP packets that contain DHCP Relay Agent Option 82 information on untrusted ports.

Use the `no` variant of this command to disable DHCP Relay Agent Option 82 information reception on untrusted ports.

**Syntax**
```plaintext
ip dhcp snooping agent-option allow-untrusted
no ip dhcp snooping agent-option allow-untrusted
```

**Default**
Disabled

**Mode**
Global Configuration

**Usage**
If the switch is connected via untrusted ports to edge switches that insert DHCP Relay Agent Option 82 information into DHCP packets, you may need to allow these DHCP packets through the untrusted ports, by using this command.

When this is disabled (default), the switch treats incoming DHCP packets on untrusted ports that contain DHCP Relay Agent Option 82 information as DHCP snooping violations: it drops them and applies any violation action specified by the `ip dhcp snooping violation` command. The switch stores statistics for packets dropped; to display these statistics, use the `show ip dhcp snooping statistics` command.

**Example**
To enable DHCP snooping Option 82 information reception on untrusted ports, use the commands:
```plaintext
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 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`
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;remote-id&gt;</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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>]
```

**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
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipaddr&gt;</code></td>
<td>Client’s IP address.</td>
</tr>
<tr>
<td><code>&lt;macaddr&gt;</code></td>
<td>Client’s MAC address in HHHH.HHHH.HHHH format.</td>
</tr>
<tr>
<td><code>&lt;vid&gt;</code></td>
<td>The VLAN ID for the entry, in the range 1 to 4094.</td>
</tr>
<tr>
<td><code>&lt;port&gt;</code></td>
<td>The port the client is connected to. The port can be a switch port, or a static or dynamic link aggregation (channel group).</td>
</tr>
<tr>
<td><code>&lt;expiry-time&gt;</code></td>
<td>The expiry time for the entry, in the range 5 to 2147483647 seconds.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Usage**
Note that dynamic entries can also be deleted from the DHCP snooping database by using the `clear ip dhcp snooping binding` command.

To add or remove static entries from the database, use the `ip source binding` command.

**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**
In a stack, the backup file is automatically synchronized across all stack members to the location configured. If the backup file is stored on a USB storage device on the stack master, it is only synchronized across stack members that also have USB storage devices installed.

If the location of the backup file is changed by using this command, a new file is created in the new location, and the old version of the file remains in the old location. This can be removed if necessary (hidden file: `.dhcp.dsn.gz`).

**Example**
To set the location of the DHCP snooping database to non-volatile storage on the switch, use the commands:
```
awplus# configure terminal
awplus(config)# ip dhcp snooping database nvs
```

**Related Commands**
`show ip dhcp snooping`
ip dhcp snooping delete-by-client

**Overview**
Use this command to set the switch to remove a dynamic entry from the DHCP snooping database when it receives a valid DHCP release message with matching IP address, VLAN ID, and client hardware address on an untrusted port, and to discard release messages that do not match an entry in the database.

Use the **no** variant of this command to set the switch to forward DHCP release messages received on untrusted ports without removing any entries from the database.

**Syntax**
```plaintext
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:
```plaintext
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:
```plaintext
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

**Usage**  If this command is enabled in a stack, and the master goes down and is replaced by a new master, entries in the DHCP snooping database for ports on the master are removed, unless they are part of link aggregators that are still up.

**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`
DHCP SNOOPING COMMANDS
IP DHCP SNOOPING MAX-BINDINGS

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-520&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

Default
The default for maximum bindings is 1.

Mode
Interface Configuration (port)

Usage
The maximum number of leases cannot be changed for a port while there are DHCP snooping Access Control Lists (ACL) associated with the port. Before using this command, remove any DHCP snooping ACLs associated with the ports. To display ACLs used for DHCP snooping, use the show ip dhcp snooping acl command.

In general, the default (1) will work well on an edge port with a single directly connected DHCP client. If the port is on an aggregation switch that is connected to an edge switch with multiple DHCP clients connected through it, then use this command to increase the number of lease entries for the port.

If there are multiple VLANs configured on the port, the limit is shared between all the VLANs on this port. For example, the default only allows one lease to be stored for one VLAN. To allow connectivity for the other VLANs, use this command to increase the number of lease entries for the port.

Example
To set the maximum number of bindings to be stored in the DHCP snooping database to 10 per port for ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# ip dhcp snooping max-bindings 10
```

Related Commands
- access-group
- show ip dhcp snooping acl
- show ip dhcp snooping interface
**DHCP SNOOPING COMMANDS**

**IP DHCP SNOOPING SUBSCRIBER-ID**

---

**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
  ```

- **Default**
  No Subscriber ID.

- **Mode**
  Interface Configuration (port)

- **Usage**
  The Subscriber ID sub-option is included in the DHCP Relay Agent Option 82 field of client DHCP packets forwarded from a port if:
  - a Subscriber ID is specified for the port using this command, and
  - DHCP snooping Option 82 information insertion is enabled (`ip dhcp snooping agent-option` command; enabled by default), and
  - DHCP snooping is enabled on the switch (`service dhcp-snooping`) and on the VLAN to which the port belongs (`ip dhcp snooping`)

- **Examples**
  To set the Subscriber ID for port 1.0.3 to `room_534`, use the commands:
  ```
  awplus# configure terminal
  awplus(config)# interface port1.0.3
  awplus(config-if)# ip dhcp snooping subscriber-id room_534
  ```
  To remove the Subscriber ID from port 1.0.3, use the commands:
  ```
  awplus# configure terminal
  awplus(config)# interface port1.0.3
  awplus(config-if)# no ip dhcp snooping subscriber-id
  ```

- **Related Commands**
  - `ip dhcp snooping agent-option`
  - `show ip dhcp snooping interface`
**ip dhcp snooping trust**

**Overview**  Use this command to set the ports to be DHCP snooping trusted ports.

Use the `no` variant of this command to return the ports to their default as untrusted ports.

**Syntax**

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

**Default**  All ports are untrusted by default.

**Mode**  Interface Configuration (port)

**Usage**  Typically, ports connecting the switch to trusted elements in the network (towards the core) are set as trusted ports, while ports connecting untrusted network elements are set as untrusted. Configure ports connected to DHCP servers as trusted ports.

**Example**  To set switch ports 1.0.1 and 1.0.2 to be trusted ports, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# ip dhcp snooping trust
```

**Related Commands**  `show ip dhcp snooping interface`
**ip dhcp snooping verify mac-address**

**Overview**  Use this command to verify that the source MAC address and client hardware address match in DHCP packets received on untrusted ports.

Use the `no` variant of this command to disable MAC address verification.

**Syntax**  
```
ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address
```

**Default**  Enabled—source MAC addresses are verified by default.

**Mode**  Global Configuration

**Usage**  When MAC address verification is enabled, the switch treats DHCP packets with source MAC address and client hardware address that do not match as DHCP snooping violations: it drops them and applies any other violation action specified by the `ip dhcp snooping violation` command. To bring the port back up again after any issues have been resolved, use the `shutdown` command.

**Example**  To disable MAC address verification on the switch, use the commands:
```
awplus# configure terminal
awplus(config)# no ip dhcp snooping verify mac-address
```

**Related Commands**  
- `ip dhcp snooping violation`
- `show ip dhcp snooping`
- `show ip dhcp snooping statistics`
**ip dhcp snooping violation**

**Overview**
Use this command to specify the action the switch will take when it detects a DHCP snooping violation by a DHCP packet on the ports.

Use the no variant of this command to disable the specified violation actions, or all violation actions.

**Syntax**
```
ip dhcp snooping violation {log|trap|link-down} ...
no ip dhcp snooping violation [{log|trap|link-down} ...]
```

**Parameter** | **Description**
--- | ---
log | Generate a log message. To display these messages, use the 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**
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>]
```

**Mode**
Global Configuration

**Usage**
This command removes static entries from the database.

To remove dynamic entries, use the `clear ip dhcp snooping binding` command or the `no` variant of the `ip dhcp snooping binding` command.

**Examples**
To add a static entry to the DHCP snooping database for a client with the IP address 192.168.1.2, MAC address 0001.0002.0003, on port1.0.6 of vlan6, use the command:
```
awplus# configure terminal
awplus(config)# ip source binding 192.168.1.2 0001.0002.0003 vlan 6 interface port1.0.6
```

To remove the static entry for IP address 192.168.1.2 from the database, use the commands:
```
awplus# configure terminal
awplus(config)# no ip source binding 192.168.1.2
```

To remove all static entries from the database, use the commands:
```
awplus# configure terminal
awplus(config)# no ip source binding
```
Related Commands

- clear ip dhcp snooping binding
- ip dhcp snooping binding
- show ip dhcp snooping binding
- show ip source binding
service dhcp-snooping

**Overview**  
Use this command to enable the DHCP snooping service globally on the switch. This must be enabled before other DHCP snooping configuration commands can be entered.

Use the `no` variant of this command to disable the DHCP snooping service on the switch. This removes all DHCP snooping configuration from the running configuration, except for any DHCP snooping maximum bindings settings (`ip dhcp snooping max-bindings` command), and any DHCP snooping-based Access Control Lists (ACLs), which are retained when the service is disabled.

**Syntax**
```
service dhcp-snooping
no service dhcp-snooping
```

**Default**  
DHCP snooping is disabled on the switch by default.

**Mode**  
Global Configuration

**Usage**  
For DHCP snooping to operate on a VLAN, it must be enabled on the switch by using this command, and also enabled on the particular VLAN by using the `ip dhcp snooping` command.

For DHCP snooping to operate on a VLAN, it must:
- be enabled globally on the switch by using this command
- be enabled on the particular VLAN by using the `ip dhcp snooping` command
- have at least one port connected to a DHCP server configured as a trusted port by using the `ip dhcp snooping trust` command

If you disable the DHCP snooping service by using the `no` variant of this command, all DHCP snooping configuration (including ARP security, but excluding maximum bindings and ACLs) is removed from the running configuration, and the DHCP snooping database is deleted from active memory. If you re-enable the service, the switch repopulates the DHCP snooping database from the dynamic lease entries in the database backup file (in NVS by default—see the `ip dhcp snooping database` command). The lease expiry times are updated.

The DHCP snooping service cannot be enabled on a switch that is configured with any of the following features, or vice versa:
- web authentication (`auth-web enable` command)
- roaming authentication (`auth roaming enable command`, `auth roaming disconnected` command)
- guest VLAN authentication (`auth guest-vlan` command)
- DHCP relay agent option (`ip dhcp-relay agent-option` command)

Any ACLs on a port that permit traffic matching DHCP snooping entries and block other traffic, will block all traffic if DHCP snooping is disabled on the port. If you disable DHCP snooping on the switch using this command, you must also remove
any DHCP snooping ACLs from the ports to maintain connectivity (no access-group command).

**Examples**

To enable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# service dhcp-snooping
```

To disable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# no service dhcp-snooping
```

**Related Commands**

- ip dhcp snooping
- ip dhcp snooping database
- ip dhcp snooping max-bindings
- show ip dhcp snooping
show arp security

**Overview**  Use this command to display ARP security configuration.

**Syntax**  `show arp security`

**Mode**  User Exec and Privileged Exec

**Example**  To display ARP security configuration on the switch use the command:

```
awplus# show arp security
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total VLANs enabled</td>
<td>The number of VLANs that have ARP security enabled.</td>
</tr>
<tr>
<td>Total VLANs disabled</td>
<td>The number of VLANs that have ARP security disabled.</td>
</tr>
</tbody>
</table>

Table 42-1: 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 42-2: Parameters in the output from the `show arp security` command

**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>]
```

**Mode**
User Exec and Privileged Exec

**Example**
To display ARP security configuration for ports, use the command:
```
awplus# show arp security interface
```

Table 42-3: Example output from the `show arp security interface` command

<table>
<thead>
<tr>
<th>Port</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.1</td>
<td>-- -- --</td>
<td>Port: Provisioned ports marked with brackets, e.g. (portx.y.z)</td>
</tr>
<tr>
<td>port1.0.2</td>
<td>-- -- --</td>
<td>KEY: LG = Log</td>
</tr>
<tr>
<td>port1.0.3</td>
<td>LG TR LD</td>
<td>TR = Trap</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>LG -- --</td>
<td>LD = Link down</td>
</tr>
<tr>
<td>port1.0.5</td>
<td>LG -- --</td>
<td></td>
</tr>
<tr>
<td>port1.0.6</td>
<td>LG TR --</td>
<td></td>
</tr>
<tr>
<td>port1.0.7</td>
<td>LG -- LD</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 42-4: Parameters in the output from the `show arp security interface` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>The action the switch takes when it detects an ARP security violation on the port.</td>
</tr>
<tr>
<td>Port</td>
<td>The port. Parentheses indicate that ports are configured for provisioning.</td>
</tr>
<tr>
<td>LG, Log</td>
<td>Generate a log message</td>
</tr>
</tbody>
</table>
### DHCP Snooping Commands

**SHOW ARP SECURITY INTERFACE**

Table 42-4: Parameters in the output from the `show arp security interface` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TR, Trap</td>
<td>Generate an SNMP notification (trap).</td>
</tr>
<tr>
<td>LD, Link down</td>
<td>Shut down the link.</td>
</tr>
</tbody>
</table>

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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Display detailed statistics.</td>
</tr>
<tr>
<td>interface &lt;port-list&gt;</td>
<td>Display statistics for the specified ports.</td>
</tr>
</tbody>
</table>

**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 42-5: Example output from the show arp security statistics command**

```
awplus# show arp security statistics
DHCP Snooping ARP Security Statistics:

<table>
<thead>
<tr>
<th>Interface</th>
<th>In Packets</th>
<th>In Discards</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.3</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>port1.0.12</td>
<td>120</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Table 42-6: Parameters in the output from the show arp security statistics command**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>A port name. Parentheses indicate that ports are configured for provisioning.</td>
</tr>
<tr>
<td>In Packets</td>
<td>The total number of incoming ARP packets that are processed by DHCP Snooping ARP Security</td>
</tr>
<tr>
<td>In Discards</td>
<td>The total number of ARP packets that are dropped by DHCP Snooping ARP Security.</td>
</tr>
</tbody>
</table>
Table 42-7: 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:

```bash
awplus# show debugging arp security
```

**Table 42-8: 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 42-9: 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 42-10: Example output from the **show ip dhcp snooping** command

<table>
<thead>
<tr>
<th>DHCP Snooping Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Snooping service ............. Enabled</td>
</tr>
<tr>
<td>Option 82 insertion ............... Enabled</td>
</tr>
<tr>
<td>Option 82 on untrusted ports ...... Not allowed</td>
</tr>
<tr>
<td>Binding delete by client .......... Disabled</td>
</tr>
<tr>
<td>Binding delete by link down ...... Disabled</td>
</tr>
<tr>
<td>Verify MAC address ............... Disabled</td>
</tr>
<tr>
<td>SNMP DHCP Snooping trap .......... Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DHCP Snooping database:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database location ................. nvs</td>
</tr>
<tr>
<td>Number of entries in database ..... 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DHCP Snooping VLANs:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total VLANs enabled .......... 1</td>
</tr>
<tr>
<td>Total VLANs disabled ............ 9</td>
</tr>
<tr>
<td>vlan1 .................. Enabled</td>
</tr>
<tr>
<td>vlan2 .................. Disabled</td>
</tr>
<tr>
<td>vlan3 .................. Disabled</td>
</tr>
<tr>
<td>vlan4 .................. Disabled</td>
</tr>
<tr>
<td>vlan5 .................. Disabled</td>
</tr>
<tr>
<td>vlan100 .............. Disabled</td>
</tr>
<tr>
<td>vlan101 .............. Disabled</td>
</tr>
<tr>
<td>vlan105 .............. Disabled</td>
</tr>
<tr>
<td>vlan1000 ............ Disabled</td>
</tr>
<tr>
<td>vlan1001 ............ Disabled</td>
</tr>
</tbody>
</table>

**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]]

**Mode**  User Exec and Privileged Exec

**Example**  To display DHCP snooping ACL information, use the command:  
awplus# show ip dhcp snooping acl

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Detailed DHCP Snooping ACL information.</td>
</tr>
<tr>
<td>hardware</td>
<td>DHCP Snooping hardware ACL information.</td>
</tr>
<tr>
<td>interface</td>
<td>ACL Interface information.</td>
</tr>
<tr>
<td>&lt;interface-list&gt;</td>
<td>The interfaces to display information about.</td>
</tr>
</tbody>
</table>

Table 42-11: Example output from the show ip dhcp snooping acl command

awplus# show ip dhcp snooping acl

DHCP Snooping Based Filters Summary:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Bindings</th>
<th>Maximum Bindings</th>
<th>Template Filters</th>
<th>Attached Hardware Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.1</td>
<td>1</td>
<td>520</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.2</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>port1.0.3</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>1</td>
<td>2</td>
<td>7</td>
<td>14</td>
</tr>
<tr>
<td>port1.0.5</td>
<td>0</td>
<td>2</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>port1.0.6</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.7</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.8</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.9</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.10</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.11</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.12</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(port2.0.1)</td>
<td>0</td>
<td>520</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(port2.0.2)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

To display DHCP snooping hardware ACL information, use the command:  
awplus# show ip dhcp snooping acl hardware
DHCP SNOOPING COMMANDS
SHOW IP DHCP SNOOPING ACL

Table 42-12: Example output from the `show ip dhcp snooping acl hardware` command

```plaintext
awplus#show ip dhcp snooping acl hardware

DHCP Snooping Based Filters in Hardware:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Access-list(/ClassMap)</th>
<th>Source IP</th>
<th>Source MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.2</td>
<td>dhcpsn1</td>
<td>10.10.10.10</td>
<td>aaaa.bbbb.cccc</td>
</tr>
<tr>
<td>port1.0.2</td>
<td>dhcpsn1</td>
<td>20.20.20.20</td>
<td>0000.aaaa.bbbb</td>
</tr>
<tr>
<td>port1.0.2</td>
<td>dhcpsn1</td>
<td>0.0.0.0</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.2</td>
<td>dhcpsn1</td>
<td>0.0.0.0</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.3</td>
<td>dhcpsn2/cmap1</td>
<td>30.30.30.30</td>
<td>aaaa.bbbb.dddd</td>
</tr>
<tr>
<td>port1.0.3</td>
<td>dhcpsn2/cmap1</td>
<td>40.40.40.40</td>
<td>0000.aaaa.cccc</td>
</tr>
<tr>
<td>port1.0.3</td>
<td>dhcpsn2/cmap1</td>
<td>50.50.50.50</td>
<td>0000.aaaa.dddd</td>
</tr>
<tr>
<td>port1.0.3</td>
<td>dhcpsn2/cmap1</td>
<td>60.60.60.60</td>
<td>0000.aaaa.eeee</td>
</tr>
<tr>
<td>port1.0.3</td>
<td>dhcpsn2/cmap1</td>
<td>70.70.70.70</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.3</td>
<td>dhcpsn2/cmap1</td>
<td>80.80.80.80</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>dhcpsn3/cmap2</td>
<td>70.70.70.70</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>dhcpsn3/cmap2</td>
<td>80.80.80.80</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>dhcpsn3/cmap2</td>
<td>70.70.70.70</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>dhcpsn3/cmap2</td>
<td>80.80.80.80</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>dhcpsn3/cmap2</td>
<td>70.70.70.70</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>dhcpsn3/cmap2</td>
<td>80.80.80.80</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>dhcpsn3/cmap2</td>
<td>70.70.70.70</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>dhcpsn3/cmap2</td>
<td>80.80.80.80</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>dhcpsn3/cmap2</td>
<td>70.70.70.70</td>
<td>0000.0000.0000</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>dhcpsn3/cmap2</td>
<td>80.80.80.80</td>
<td>0000.0000.0000</td>
</tr>
</tbody>
</table>
```

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 42-13: Example output from the `show ip dhcp snooping acl detail interface` command

```plaintext
awplus#show ip dhcp snooping acl detail interface port1.0.4

DHCP Snooping Based Filters Information:

port1.0.4 : Maximum Bindings ........... 2
port1.0.4 : Template filters .......... 7
port1.0.4 : Attached hardware filters .. 14
port1.0.4 : Current bindings .......... 1, 1 free
port1.0.4 : Client 1 ............... 120.120.120.120
port1.0.4 : Templates: cheese (via class-map: cmap2)
port1.0.4 :  10 permit ip dhcpsnooping 100.0.0.0/8
port1.0.4 : Template: dhcpsn2 (via class-map: cmap1)
port1.0.4 :  10 permit ip dhcpsnooping any
port1.0.4 :  20 permit ip dhcpsnooping 10.0.0.0/8
port1.0.4 :  30 permit ip dhcpsnooping 20.0.0.0/8
port1.0.4 :  40 permit ip dhcpsnooping 30.0.0.0/8
port1.0.4 : Template: dhcpsn1 (via access-group)
port1.0.4 :  10 permit ip dhcpsnooping any mac dhcpsnooping abcd.0000.0000 00 00.ffff.ffff
port1.0.4 :  20 permit ip dhcpsnooping any
```
Related Commands

access-list hardware (named)
show access-list (IPv4 Hardware ACLs)
show ip dhcp snooping agent-option

**Overview**  Use this command to display DHCP snooping Option 82 information for all interfaces, a specific interface or a range of interfaces.

**Syntax**  
```
show ip dhcp snooping agent-option [interface <interface-list>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specify the interface.</td>
</tr>
<tr>
<td>&lt;interface-list&gt;</td>
<td>The name of the interface or interface range.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Examples**  To display DHCP snooping Option 82 information for all interfaces, use the command:
```
awplus# show ip dhcp snooping agent-option
```
To display DHCP snooping Option 82 information for port1.0.1, use the command:
```
awplus# show ip dhcp snooping agent-option interface port1.0.1
```
To display DHCP snooping Option 82 information for vlan1, use the command:
```
awplus# show ip dhcp snooping agent-option interface vlan1
```
To display DHCP snooping Option 82 information for port2.0.1, port4.0.2 and ports in the range from port4.0.10 to port4.0.15, use the command:
```
awplus# show ip dhcp snooping agent-option interface port2.0.1, port4.0.2, port4.0.10-port4.0.15
```
DHCP Snooping Commands
SHOW IP DHCP SNOOPING AGENT-OPTION

Output

Figure 42-1: 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
```

```
show ip dhcp snooping agent-option

DHCP Snooping Option 82 Configuration:

Key: C Id = Circuit Id Format
     R Id = Remote Id
     S Id = Subscriber Id

Option 82 insertion ............... Enabled
Option 82 on untrusted ports ...... Not allowed

vlan1  C Id = vlanifindex
       R Id = Access-Island-01-M1
vlan2  C Id = vlantriplet
       R Id = Access-Island-01-M1
vlan3  C Id = vlantriplet
       R Id = Access-Island-01-M3
vlan4  C Id = vlantriplet
       R Id = 0000.cd28.074c
vlan5  C Id = vlantriplet
       R Id = 0000.cd28.074c
vlan6  C Id = vlantriplet
       R Id = 0000.cd28.074c
port1.1.1 S Id =
port1.1.2 S Id =
port1.1.3 S Id = phone_1
port1.1.4 S Id =
port1.1.5 S Id =
port1.1.6 S Id = phone_2
port1.1.7 S Id = PC_1
port1.1.8 S Id =
port1.1.9 S Id =
port1.1.10 S Id =
port1.1.11 S Id =
port1.1.12 S Id =

Related Commands:

ip dhcp snooping agent-option
ip dhcp snooping agent-option circuit-id vlantriplet
ip dhcp snooping agent-option remote-id
ip dhcp snooping subscriber-id
show ip dhcp snooping
show ip dhcp snooping interface
show ip dhcp snooping binding

**Overview**  Use this command to display all dynamic and static entries in the DHCP snooping binding database.

**Syntax**  show ip dhcp snooping binding

**Mode**  User Exec and Privileged Exec

**Example**  To display entries in the DHCP snooping database, use the command:

```
awplus# show ip dhcp snooping binding
```

<p>| Table 42-14: Example output from the <strong>show ip dhcp snooping binding</strong> command |
|---------------------------------|--------|--------------|--------|--------------|---|---|</p>
<table>
<thead>
<tr>
<th>Client IPAddress</th>
<th>MAC Address</th>
<th>Server IPAddress</th>
<th>VLAN</th>
<th>Port</th>
<th>Expires (sec)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.4</td>
<td>aaaa.bbbb.cccc</td>
<td>--</td>
<td>7</td>
<td>1.0.6</td>
<td>Infinite</td>
<td>Stat</td>
</tr>
<tr>
<td>1.2.3.6</td>
<td>any</td>
<td>--</td>
<td>4077</td>
<td>1.0.6</td>
<td>Infinite</td>
<td>Stat</td>
</tr>
<tr>
<td>1.3.4.5</td>
<td>any</td>
<td>--</td>
<td>1</td>
<td>sal</td>
<td>Infinite</td>
<td>Stat</td>
</tr>
<tr>
<td>111.111.100.101</td>
<td>0000.0000.0001</td>
<td>111.112.1.1</td>
<td>1</td>
<td>1.0.6</td>
<td>4076</td>
<td>Dyna</td>
</tr>
<tr>
<td>111.111.101.108</td>
<td>0000.0000.0108</td>
<td>111.112.1.1</td>
<td>1</td>
<td>1.0.6</td>
<td>4084</td>
<td>Dyna</td>
</tr>
<tr>
<td>111.111.101.109</td>
<td>0000.0000.0109</td>
<td>111.112.1.1</td>
<td>1</td>
<td>1.0.6</td>
<td>4085</td>
<td>Dyna</td>
</tr>
<tr>
<td>111.211.100.101</td>
<td>--</td>
<td>--</td>
<td>1</td>
<td>1.0.2</td>
<td>2147483325</td>
<td>Dyna</td>
</tr>
<tr>
<td>111.211.100.109</td>
<td>00b0.0000.0009</td>
<td>111.112.111.111</td>
<td>1</td>
<td>1.0.2</td>
<td>21</td>
<td>Dyna</td>
</tr>
<tr>
<td>111.211.101.101</td>
<td>00b0.0000.0101</td>
<td>111.112.111.111</td>
<td>1</td>
<td>1.0.2</td>
<td>214</td>
<td>Dyna</td>
</tr>
</tbody>
</table>

Total number of bindings in database: 9

| Table 42-15: Parameters in the output from the **show ip dhcp snooping binding** command |
|---------------------------------|--------|----------------|
| **Parameter**                   | **Description**                              |
| Client IPAddress | The IP address of the DHCP client. |
| MAC Address | The MAC address of the DHCP client. |
| Server IP | The IP address of the DHCP server. |
| VLAN | The VLAN associated with this entry. |
| Port | The port the client is connected to. |
| Expires (sec) | The time in seconds until the lease expires. |
DHCP SNOOPING COMMANDS
SHOW IP DHCP SNOOPING BINDING

Table 42-15: Parameters in the output from the show ip dhcp snooping binding command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The source of the entry:</td>
</tr>
<tr>
<td></td>
<td>• Dyna: dynamically entered by snooping DHCP traffic, configured by the ip dhcp snooping binding command, or loaded from the database backup file.</td>
</tr>
<tr>
<td></td>
<td>• Stat: added statically by the ip source binding command</td>
</tr>
<tr>
<td>Total number of bindings in database</td>
<td>The total number of dynamic and static lease entries in the DHCP snooping database.</td>
</tr>
</tbody>
</table>

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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports to display DHCP snooping configuration information for. If no ports are specified, information for all ports is displayed.</td>
</tr>
</tbody>
</table>

**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 42-16: Example output from the **show ip dhcp snooping interface** command

```
awplus# show ip dhcp snooping interface

DHCP Snooping Port Status and Configuration:

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Full Leases</th>
<th>Max Leases</th>
<th>Action</th>
<th>Subscriber-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>port1.0.1</td>
<td>Untrusted</td>
<td>1</td>
<td>1</td>
<td>LG</td>
<td>--</td>
</tr>
<tr>
<td>port1.0.2</td>
<td>Untrusted</td>
<td>0</td>
<td>50</td>
<td>LG</td>
<td>TR LD</td>
</tr>
<tr>
<td>port1.0.3</td>
<td>Untrusted</td>
<td>0</td>
<td>50</td>
<td>LG</td>
<td>--</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>Untrusted</td>
<td>0</td>
<td>50</td>
<td>LG</td>
<td>--</td>
</tr>
<tr>
<td>port1.0.5</td>
<td>Untrusted</td>
<td>0</td>
<td>50</td>
<td>LG</td>
<td>LD</td>
</tr>
<tr>
<td>port1.0.6</td>
<td>Untrusted</td>
<td>0</td>
<td>1</td>
<td>LG</td>
<td>--</td>
</tr>
<tr>
<td>port1.0.7</td>
<td>Untrusted</td>
<td>0</td>
<td>1</td>
<td>LG</td>
<td>--</td>
</tr>
<tr>
<td>port1.0.8</td>
<td>Untrusted</td>
<td>0</td>
<td>1</td>
<td>LG</td>
<td>--</td>
</tr>
<tr>
<td>port1.0.9</td>
<td>Untrusted</td>
<td>0</td>
<td>1</td>
<td>--</td>
<td>TR</td>
</tr>
<tr>
<td>port1.0.10</td>
<td>Untrusted</td>
<td>0</td>
<td>1</td>
<td>--</td>
<td>-- LD</td>
</tr>
<tr>
<td>port1.0.11</td>
<td>Trusted</td>
<td>0</td>
<td>1</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>port1.0.12</td>
<td>Trusted</td>
<td>0</td>
<td>1</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>
```
Table 42-17: Parameters in the output from the `show ip dhcp snooping interface` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port interface name.</td>
</tr>
<tr>
<td>Status</td>
<td>The port status: untrusted (default) or trusted.</td>
</tr>
<tr>
<td>Full Leases</td>
<td>The number of entries in the DHCP snooping database for the port.</td>
</tr>
<tr>
<td>Max Leases</td>
<td>The maximum number of entries that can be stored in the database for the port.</td>
</tr>
<tr>
<td>Action</td>
<td>The DHCP snooping violation actions for the port.</td>
</tr>
<tr>
<td>Subscriber ID</td>
<td>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 <code>show running-config dhcp</code> command.</td>
</tr>
</tbody>
</table>

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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Display detailed statistics.</td>
</tr>
<tr>
<td>interface &lt;interface-list&gt;</td>
<td>Display statistics for the specified interfaces. The interface list can contain switch ports, static or dynamic link aggregators (channel groups), or VLANs.</td>
</tr>
</tbody>
</table>

**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 42-18: Example output from the show ip dhcp snooping statistics command**

<table>
<thead>
<tr>
<th>Interface</th>
<th>In Packets</th>
<th>In BOOTP Requests</th>
<th>In BOOTP Replies</th>
<th>In Discards</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan1</td>
<td>444</td>
<td>386</td>
<td>58</td>
<td>223</td>
</tr>
<tr>
<td>port1.0.1</td>
<td>386</td>
<td>386</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>port1.0.6</td>
<td>58</td>
<td>0</td>
<td>58</td>
<td>0</td>
</tr>
</tbody>
</table>
Table 42-19: Example output from the `show ip dhcp snooping statistics detail` command

```
awplus# show ip dhcp snooping statistics detail
DHCP Snooping Statistics:
Interface ........................................ port1.0.1, All counters 0
Interface ........................................ port1.0.2, All counters 0
Interface ........................................ port1.0.3, All counters 0
Interface ........................................ port1.0.4
  In Packets ..................................... 50
  In BOOTP Requests ............................ 25
  In BOOTP Replies ............................. 25
  In Discards .................................... 1
  Invalid BOOTP Information .................... 0
  Invalid DHCP ACK ............................ 0
  Invalid DHCP Release or Decline ............. 0
  Invalid IP/UDP Header ....................... 0
  Max Bindings Exceeded ....................... 1
  Option 82 Insert Error ....................... 0
  Option 82 Received Invalid ................. 0
  Option 82 Received On Untrusted Port ...... 0
  Option 82 Transmit On Untrusted Port ...... 0
  Reply Received On Untrusted Port .......... 0
  Source MAC/CHADDR Mismatch ............... 0
  Static Entry Already Exists ............... 0
Interface ........................................ port1.0.5, All counters 0
Interface ........................................ port1.0.6, All counters 0
```

Table 42-20: Parameters in the output from the `show ip dhcp snooping statistics` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface name.</td>
</tr>
<tr>
<td>In Packets</td>
<td>The total number of incoming packets that are processed by DHCP Snooping.</td>
</tr>
<tr>
<td>In BOOTP Requests</td>
<td>The total number of incoming BOOTP Requests.</td>
</tr>
<tr>
<td>In BOOTP Replies</td>
<td>The total number of incoming BOOTP Replies.</td>
</tr>
<tr>
<td>In Discards</td>
<td>The total number of incoming packets that have been discarded.</td>
</tr>
<tr>
<td>Invalid BOOTP Information</td>
<td>Packet contained invalid BOOTP information, such as an invalid BOOTP.OPCode.</td>
</tr>
<tr>
<td>Invalid DHCP ACK</td>
<td>A DHCP ACK message was discarded, for reasons such as missing Server Option or Lease Option.</td>
</tr>
<tr>
<td>Invalid DHCP Release or Decline</td>
<td>A DHCP Release or Decline message was discarded, for reasons such as mismatch between received interface and current binding information.</td>
</tr>
</tbody>
</table>
DHCP SNOOPING COMMANDS
SHOW IP DHCP SNOOPING STATISTICS

Table 42-20: Parameters in the output from the `show ip dhcp snooping statistics` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid IP/UDP Header</td>
<td>A problem was detected in the IP or UDP header of the packet.</td>
</tr>
<tr>
<td>Max Bindings Exceeded</td>
<td>Accepting the packet would cause the maximum number of bindings on a port to be exceeded.</td>
</tr>
<tr>
<td>Option 82 Insert Error</td>
<td>An error occurred while trying to insert DHCP Relay Agent Option 82 information.</td>
</tr>
<tr>
<td>Option 82 Received Invalid</td>
<td>The DHCP Relay Agent Option 82 information received did not match the information inserted by DHCP Snooping.</td>
</tr>
<tr>
<td>Option 82 Received On Untrusted Port</td>
<td>A packet containing DHCP Relay Agent Option 82 information was received on an untrusted port.</td>
</tr>
<tr>
<td>Option 82 Transmit On Untrusted Port</td>
<td>A packet containing DHCP Relay Agent Option 82 information was to be sent on an untrusted port.</td>
</tr>
<tr>
<td>Reply Received On Untrusted Port</td>
<td>A BOOTP reply was received on an untrusted port.</td>
</tr>
<tr>
<td>Source MAC/CHADDR Mismatch</td>
<td>The L2 Source MAC address of the packet did not match the client hardware address field (BOOTP.CHADDR).</td>
</tr>
<tr>
<td>Static Entry Already Exists</td>
<td>An entry could not be added as a static entry already exists.</td>
</tr>
</tbody>
</table>

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 42-21: Example output from the `show ip source binding` command**

<table>
<thead>
<tr>
<th>Client IP Address</th>
<th>MAC Address</th>
<th>VLAN</th>
<th>Port</th>
<th>Expires (sec)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>0000.1111.2222</td>
<td>1</td>
<td>port1.0.1</td>
<td>Infinite</td>
<td>Static</td>
</tr>
</tbody>
</table>

**Table 42-22: Parameters in the output from the `show ip source binding` command**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client IP Address</td>
<td>The IP address of the DHCP client.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the DHCP client.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN ID the packet is received on.</td>
</tr>
<tr>
<td>Port</td>
<td>The Layer 2 port name the packet is received on.</td>
</tr>
<tr>
<td>Expires (sec)</td>
<td>Always infinite for static bindings, or when the leave time in the DHCP message was 0xffffffff (infinite).</td>
</tr>
<tr>
<td>Type</td>
<td>DHCP Snooping binding type: Static</td>
</tr>
</tbody>
</table>

**Related Commands**
- `ip source binding`
- `show ip dhcp snooping binding`
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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.
VRRP COMMANDS

Command List

- “advertisement-interval” on page 1814
- “circuit-failover” on page 1816
- “debug vrrp” on page 1818
- “debug vrrp events” on page 1819
- “debug vrrp packet” on page 1820
- “disable (VRRP)” on page 1821
- “enable (VRRP)” on page 1822
- “preempt-mode” on page 1823
- “priority” on page 1825
- “router vrrp (interface)” on page 1827
- “router ipv6 vrrp (interface)” on page 1828
- “show debugging vrrp” on page 1829
- “show running-config router vrrp” on page 1830
- “show running-config router ipv6 vrrp” on page 1831
- “show vrrp” on page 1832
- “show vrrp ipv6” on page 1834
- “show vrrp counters” on page 1835
- “show vrrp (session)” on page 1838
- “transition-mode” on page 1840
- “undebug vrrp” on page 1842
- “undebug vrrp events” on page 1843
- “undebug vrrp packet” on page 1844
- “virtual-ip” on page 1845
- “virtual-ipv6” on page 1847
- “vrrp vmac” on page 1849
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
```

**Default**  
The default advertisement interval is 1 second.

**Mode**  
Router Configuration

**Usage**  
Note when using VRRP with VCStacking, ensure the VRRP advertisement-interval is larger than the VCStacking failover time to avoid VCStacking failovers causing VRRP failovers.

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

**NOTE:**

When using VRRPv3 with VCStacking, ensure that the VRRPv3 advertisement-interval is configured to a longer time than the VCStacking failover time.

If the VRRPv3 advertisement-interval is shorter than the VCStacking failover time, then a VRRPv3 failover will also occur whenever a VCStacking failover occurs. Use seconds not centiseconds to ensure interoperability with VRRPv2.
VRRP COMMANDS

ADVERTISEMENT-INTERVAL

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:

```plaintext
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:

```plaintext
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:

```plaintext
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)`
circuit-failover

**Overview**
Use this command to enable the VRRP circuit failover feature. See 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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>The interface of the router that is monitored. 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.</td>
</tr>
<tr>
<td>&lt;1-253&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Mode**
Router Configuration

**Examples**
The example below shows you how to configure circuit failover on interface vlan2 for the VRRP IPv4 session with VR ID 1, where interface vlan2 is considered the monitored interface:

awplus# configure terminal
awplus(config)# router vrrp 1 vlan2
awplus(config-router)# circuit-failover vlan2 30

The example below shows you how to remove all configured circuit failovers for the VRRP IPv4 session with VR ID 1 on interface vlan2:

awplus# configure terminal
awplus(config)# router vrrp 1 vlan2
awplus(config-router)# no circuit-failover

The example below shows you how to configure circuit failover on interface vlan2 for the VRRPv3 IPv6 session with VR ID 2, where interface vlan2 is considered the monitored interface:

awplus# configure terminal
awplus(config)# router ipv6 vrrp 2 vlan2
awplus(config-router)# circuit-failover vlan2 30
The example below shows you how to remove all configured circuit failovers for the VRRPv3 IPv6 session with VR ID 1 on interface vlan2:

```
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]
nod debug vrrp [all]
```

**Mode**  Privileged Exec and Global Configuration

**Usage**  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**  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]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>send</td>
<td>Specifies the debug option set for sent packets.</td>
</tr>
<tr>
<td>recv</td>
<td>Specifies the debug option set for received packets.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec and Global Configuration

**Usage**
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**  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 any 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**
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**
The example below shows you how to enable the VRRP session for VRRP VR ID 5 on vlan2:
```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# enable
```

The example below shows you how to enable the VRRPv3 session for VRRPv3 VR ID 3 on vlan1:
```
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.

**Syntax**  `preempt-mode {true|false}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>Preemption is enabled.</td>
</tr>
<tr>
<td>false</td>
<td>Preemption is disabled.</td>
</tr>
</tbody>
</table>

**Default**  The default is `true`.

**Mode**  Router Configuration

**Usage**  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 on `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 take over for the backup virtual router that was elected to become the master virtual router.

This preemptive scheme can be disabled using the `preempt-mode false` command. If preemption is disabled, the backup virtual router that is currently elected as the master virtual router does not transition to backup virtual router again whenever the alternate backup router with a higher priority becomes available.

See the VRRP Feature Overview and Configuration Guide for more information about:

- VRRPv3 IPv4 configuration details
- VRRPv3 IPv6 configuration details
- preempt mode

**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

**Related Commands**

- circuit-failover
- priority
- router vrrp (interface)
- router ipv6 vrrp (interface)
**VRRP COMMANDS**

**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-255&gt;</code></td>
<td>The priority. For the master router, use 255 for this parameter; otherwise use any number from the range <code>&lt;1-254&gt;</code>.</td>
</tr>
</tbody>
</table>

**Default**
Defaults for priority are: `master router` = 255; `backup` = 100.

**Mode**
Router Configuration

**Usage**
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 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>

Example
The example below shows you how to enable a VRRP session with VR ID 5 on vlan1:
awplus# configure terminal
awplus(config)# router vrrp 5 vlan1
awplus(config-router)# enable
awplus(config-router)#

The example below shows you how to disable a VRRP session with VR ID 5 on vlan1:
awplus(config-router)# disable
awplus(config-router)# exit
awplus(config)# no router vrrp 5 vlan1
awplus(config)#

Mode
Global Configuration

Usage
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.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

Examples

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vrid&gt;</td>
<td>&lt;1-255&gt; The ID of the virtual router VRRP IPv4 session to create.</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>Specify the name of the interface that will participate in the virtual routing. The interface specified sends and receives VRRP IPv4 advertisement messages.</td>
</tr>
</tbody>
</table>

Related Commands
advertisement-interval
circuit-failover
disable (VRRP)
enable (VRRP)
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**
- `<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**
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.

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`
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 “Controlling “show” Command Output” in 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 vrrp

**Overview** Use this command to show the running configuration for VRRP IPv4.

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.

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 43-1: 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 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 “Controlling “show” Command Output” in 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 43-2:  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 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 “Controlling “show” Command Output” in 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]
```

**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 43-3:  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 43-4:  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
```
VRRP COMMANDS
SHOW VRRP

**Related Commands**

- enable (VRRP)
- disable (VRRP)
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 “Controlling “show” Command Output” in 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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**  To display information about all VRRPv3 IPv6 sessions, enter the command:

```
awplus# show vrrp ipv6
```

**Output**  Figure 43-5:  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 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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

For VRRPv3 IPv4 configuration details, see the VRRP Feature Overview and Configuration Guide.

**Syntax**  show vrrp counters

**Mode**  User Exec and Privileged Exec

**Usage**  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 43-6: 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 43-1: Global counters with descriptions for the `show vrrp counters` command:

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checksum Errors</td>
<td>The total number of VRRP packets received with an invalid VRRP checksum value.</td>
</tr>
<tr>
<td>Version Errors</td>
<td>The total number of VRRP packets received with an unknown or unsupported version number.</td>
</tr>
<tr>
<td>VRID Errors</td>
<td>The total number of VRRP packets received with an invalid VRID for this virtual router.</td>
</tr>
</tbody>
</table>

Table 43-2: Per VR counters with descriptions for the `show vrrp counters` command:

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Transitions</td>
<td>The total number of times that this virtual router’s state has transitioned to MASTER.</td>
</tr>
<tr>
<td>Received Advertisements</td>
<td>The total number of VRRP advertisements received by this virtual router.</td>
</tr>
</tbody>
</table>
Table 43-2: Per VR counters with descriptions for the `show vrrp counters` command: (cont.)

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Errors</td>
<td>The total number of VRRP advertisement packets received for which the advertisement interval is different than the one configured for the local virtual router.</td>
</tr>
<tr>
<td>TTL Errors</td>
<td>The total number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.</td>
</tr>
<tr>
<td>Received Priority 0 Pkt</td>
<td>The total number of VRRP packets received by the virtual router with a priority of '0'.</td>
</tr>
<tr>
<td>Sent Priority 0 Pkt</td>
<td>The total number of VRRP packets sent by the virtual router with a priority of '0'.</td>
</tr>
<tr>
<td>Received Invalid Type</td>
<td>The number of VRRP packets received by the virtual router with an invalid value in the 'type' field.</td>
</tr>
<tr>
<td>Address List Errors</td>
<td>The total number of packets received for which the address list does not match the locally configured list for the virtual router.</td>
</tr>
<tr>
<td>Packet Length Errors</td>
<td>The total number of packets received with a packet length less than the length of the VRRP header.</td>
</tr>
<tr>
<td>Monitored Circuit Up</td>
<td>The total number of times the monitored circuit has generated the UP event.</td>
</tr>
<tr>
<td>Monitored Circuit Down</td>
<td>The total number of times the monitored circuit has generated the down event.</td>
</tr>
</tbody>
</table>
show vrrp (session)

**Overview**  
Use this command to display information for a particular VRRP session.  
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.  
See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

**Syntax**  
show vrrp <vrid> <interface>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vrid&gt;</td>
<td>&lt;1-255&gt; The virtual router ID for which to display information. Session must already exist.</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>The interface to display information about, for instance, vlan2.</td>
</tr>
</tbody>
</table>

**Mode**  
User Exec and Privileged Exec

**Usage**  
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
```
**Example**

The following command shows information about VRRP session 5 for interface vlan2.

```
awplus# show vrrp 5 vlan2
```

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
**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}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>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.</td>
</tr>
<tr>
<td>false</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Default**  The default is **false**.

**Mode**  Router Configuration

**Usage**  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)`
**debug 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`
**Overview**  
Use this command to disable debugging options for VRRP packets.

**Syntax**  
undebug vrrp packet [send|recv]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>send</td>
<td>Disable the debug option set for sent packets.</td>
</tr>
<tr>
<td>recv</td>
<td>Disable the debug option set for received packets.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec

**Examples**  
The example below shows you how to disable VRRP sent packet debugging:

```bash
awplus# undebug vrrp packet send
```

The example below shows you how to disable VRRP received packet debugging:

```bash
awplus# undebug vrrp packet recv
```

The example below shows you how to disable all VRRP packet debugging:

```bash
awplus# undebug vrrp packet
```

**Related Commands**  
dump 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]
```

```
o virtual-ip
```

**Mode**  Router Configuration

**Usage**  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 `vrp 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipv6-address&gt;</td>
<td>The IPv6 address of the virtual router, entered in hexadecimal, in the format X:X::X.X.</td>
</tr>
<tr>
<td>master</td>
<td>Sets <strong>master</strong> to be the default state of the VRRPv3 router within the Virtual Router. For <strong>master</strong>, the router must own the Virtual IP address.</td>
</tr>
<tr>
<td>backup</td>
<td>Sets <strong>backup</strong> to be the default state of the VRRPv3 router within the Virtual Router.</td>
</tr>
<tr>
<td>primary</td>
<td>Sets the specified address as the primary IPv6 address. The primary address must be a link-local IPv6 address.</td>
</tr>
<tr>
<td>secondary</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Mode**  Router Configuration

**Usage**  The VRRP master and owner of the virtual IPv6 address for the VRRPv3 session only responds to the packets destined to the virtual IPv6 address. The VRRP master that is not an owner of the virtual IPv6 address for the VRRPv3 session does not respond to the packets destined to the virtual IPv6 address, but forwards packets with a VMAC as the destination address. See the **vrp vmac** command to enable and disable this feature.

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
Introduction

Overview  This chapter provides an alphabetical reference for commands used to configure EPSR. For more information, see the EPSR Feature Overview and Configuration Guide.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.
**Command List**

- “debug epsr” on page 1851
- “epsr” on page 1852
- “epsr configuration” on page 1854
- “epsr datavlan” on page 1855
- “epsr enhancedrecovery enable” on page 1856
- “epsr mode master controlvlan primary port” on page 1857
- “epsr mode transit controlvlan” on page 1858
- “epsr priority” on page 1859
- “epsr state” on page 1860
- “epsr trap” on page 1861
- “show debugging epsr” on page 1862
- “show epsr” on page 1863
- “show epsr common segments” on page 1868
- “show epsr config-check” on page 1869
- “show epsr <epsr-instance>” on page 1871
- “show epsr <epsr-instance> counters” on page 1872
- “show epsr counters” on page 1873
- “show epsr summary” on page 1874
- “undebug epsr” on page 1875
**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}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>info</code></td>
<td>Send general EPSR information to the console. Using this parameter with the <strong>no debug epsr</strong> command will explicitly exclude the above information from being sent to the console.</td>
</tr>
<tr>
<td><code>msg</code></td>
<td>Send the decoded received and transmitted EPSR packets to the console. Using this parameter with the <strong>no debug epsr</strong> command will explicitly exclude the above packets from being sent to the console.</td>
</tr>
<tr>
<td><code>pkt</code></td>
<td>Send the received and transmitted EPSR packets as raw ASCII text to the console. Using this parameter with the <strong>no debug epsr</strong> command will explicitly exclude the above packets from being sent to the console.</td>
</tr>
<tr>
<td><code>state</code></td>
<td>Send EPSR state transitions to the console. Using this parameter with the <strong>no debug epsr</strong> command will explicitly exclude state transitions from being sent to the console.</td>
</tr>
<tr>
<td><code>timer</code></td>
<td>Send EPSR timer information to the console. Using this parameter with the <strong>no debug epsr</strong> command will explicitly exclude timer information from being sent to the console.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Send all EPSR debugging information to the console. Using this parameter with the <strong>no debug epsr</strong> command will explicitly exclude any debugging information from being sent to the console.</td>
</tr>
</tbody>
</table>

**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`
**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 Premium License.

**Syntax**

```plaintext
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.

**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
```

*NOTE:* When stacking is used with EPSR, the EPSR failovertime should be at least 5 seconds.

To delete the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)#
```
**Related Commands**

- `epsr mode master controlvlan primary port`
- `epsr mode transit controlvlan`
- `epsr configuration`
- `epsr datavlan`
- `epsr state`
- `epsr trap`
- `reboot rolling`
- `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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;epsr-instance&gt;</td>
<td>Name of the EPSR instance.</td>
</tr>
<tr>
<td>datavlan</td>
<td>Adds a data VLAN to be protected by the EPSR instance.</td>
</tr>
<tr>
<td>&lt;vlanid&gt;</td>
<td>The VLAN’s VID - a number between 1 and 4094 excluding the number selected for the control VLAN.</td>
</tr>
<tr>
<td>&lt;vlanid-range&gt;</td>
<td>Specify a range of VLAN identifiers using a hyphen to separate identifiers.</td>
</tr>
</tbody>
</table>

**Mode**
EPSR Configuration

**Usage**
We recommend you

- set the EPSR control VLAN to vlan2, using the **epsr mode master controlvlan primary port** and **epsr mode transit controlvlan** commands, then
- set the EPSR data VLAN between to be a value between 3 and 4094, using the **epsr datavlan** command.

**Examples**
To add **vlan3** to the EPSR instance called **blue**, use the command:
```
awplus(config-epsr)# epsr blue datavlan vlan3
```
To add **vlan2 and vlan3** to the EPSR instance called **blue**, use the command:
```
awplus(config-epsr)# epsr blue datavlan vlan2-vlan3
```
To remove **vlan3** from the EPSR instance called **blue**, use the command:
```
awplus(config-epsr)# no epsr blue datavlan vlan3
```
To remove **vlan2 and vlan3** from the EPSR instance called **blue**, use the command:
```
awplus(config-epsr)# no epsr blue datavlan vlan2-vlan3
```

**Related Commands**
- **epsr mode master controlvlan primary port**
- **epsr mode transit controlvlan**
- **show epsr**
### epsr enhancedrecovery enable

#### Overview
This command enables EPSR’s enhanced recovery mode. Enhanced recovery mode enables a ring to apply additional recovery procedures when a ring with more than one break partially mends. For more information, see the EPSR Feature Overview and Configuration Guide.

The `no` variant of this command disables the enhanced recovery mode.

#### Syntax
```
epsr <epsr-instance> enhancedrecovery enable
no epsr <epsr-instance> enhancedrecovery enable
```

#### Default
Default is that enhanced recovery mode disabled.

#### Mode
EPSR Configuration

#### Example
To apply enhanced recovery on the EPSR instance called `blue`, use the command:
```
awplus(config-epsr)# epsr blue enhancedrecovery enable
```

#### Related Commands
`show epsr`
## EPSR MODE MASTER CONTROLVLAN PRIMARY PORT

### Overview

This command creates a master EPSR instance.

**NOTE:** Running your switch as an EPSR master node requires a Premium License.

### Syntax

```
epsr <epsr-instance> mode master controlvlan <2-4094> primaryport <port>
```

### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;epsr-instance&gt;</td>
<td>Name of the EPSR instance.</td>
</tr>
<tr>
<td>mode</td>
<td>Determines the node is acting as a master.</td>
</tr>
<tr>
<td>master</td>
<td>Sets switch to be the master node for the named EPSR ring.</td>
</tr>
<tr>
<td>controlvlan</td>
<td>The VLAN that will transmit EPSR control frames.</td>
</tr>
<tr>
<td>&lt;2-4094&gt;</td>
<td>VLAN id.</td>
</tr>
<tr>
<td>primaryport</td>
<td>Primary port for the EPSR instance.</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td>The primary port. The port may be a switch port (e.g. port1.0.4) or a static channel group (e.g. sa2). It cannot be a dynamic (LACP) channel group.</td>
</tr>
</tbody>
</table>

**NOTE:**

The software allows you to configure more than two ports or static channel groups to the control VLAN within a single switch or stacked node. 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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;epsr-instance&gt;</td>
<td>Name of the EPSR instance.</td>
</tr>
<tr>
<td>mode</td>
<td>Determines the node is acting as a transit node.</td>
</tr>
<tr>
<td>transit</td>
<td>Sets switch to be the transit node for the named EPSR ring.</td>
</tr>
<tr>
<td>controlvlan</td>
<td>The VLAN that will transmit EPSR control frames.</td>
</tr>
<tr>
<td>&lt;2-4094&gt;</td>
<td>VLAN id.</td>
</tr>
</tbody>
</table>

**NOTE:** The software allows you to configure more than two ports or static channel groups to the control VLAN within a single switch or stacked node. 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;epsr-instance&gt;</td>
<td>Name of the EPSR instance.</td>
</tr>
<tr>
<td>priority</td>
<td>The priority of the ring instance selected by the epsr-name parameter.</td>
</tr>
<tr>
<td>&lt;0-127&gt;</td>
<td>The priority to be applied (0 is the lowest priority and represents no superloop protection).</td>
</tr>
</tbody>
</table>

**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}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;epsr-instance&gt;</td>
<td>The name of the EPSR instance.</td>
</tr>
<tr>
<td>state</td>
<td>The operational state of the ring.</td>
</tr>
<tr>
<td>enabled</td>
<td>EPSR instance is enabled.</td>
</tr>
<tr>
<td>disabled</td>
<td>EPSR instance is disabled.</td>
</tr>
</tbody>
</table>

**Mode**  EPSR Configuration

**Example**  To enable the EPSR instance called blue, use the command:
```
awplus(config-epsr)# epsr blue state enabled
```

**Related Commands**  
- epsr mode master controlvlan primary port
- epsr mode transit controlvlan
epsr trap

**Overview**  This command enables SNMP traps for an EPSR instance. The traps will be sent when the EPSR instance changes state.

The **no** variant of this command disables SNMP traps for an EPSR instance. The traps will no longer be sent when the EPSR instance changes state.

**Syntax**

```
epsr <epsr-instance> trap
no epsr <epsr-instance> trap
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;epsr-instance&gt;</td>
<td>Name of the EPSR instance.</td>
</tr>
<tr>
<td>trap</td>
<td>SNMP trap for the EPSR instance.</td>
</tr>
</tbody>
</table>

**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:**  
The following examples show the output display for a non-superloop topology network.

<table>
<thead>
<tr>
<th>EPSR Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name .................. test2</td>
</tr>
<tr>
<td>Mode .................... Transit</td>
</tr>
<tr>
<td>Status .................. Enabled</td>
</tr>
<tr>
<td>State .................... Links-Up</td>
</tr>
<tr>
<td>Control Vlan .......... 2</td>
</tr>
<tr>
<td>Data VLAN(s) .......... 10</td>
</tr>
<tr>
<td>Interface Mode ................ Ports Only</td>
</tr>
<tr>
<td>First Port ................. port1.0.1</td>
</tr>
<tr>
<td>First Port Status ........... Down</td>
</tr>
<tr>
<td>First Port Direction ........ Unknown</td>
</tr>
<tr>
<td>Second Port ............... port1.0.2</td>
</tr>
<tr>
<td>Second Port Status ........ Down</td>
</tr>
<tr>
<td>Second Port Direction .... Unknown</td>
</tr>
<tr>
<td>Trap ........................ Enabled</td>
</tr>
<tr>
<td>Master Node ............... Unknown</td>
</tr>
<tr>
<td>Enhanced Recovery ........ Disabled</td>
</tr>
</tbody>
</table>

---

**Table 44-1:** Example output from the `show epsr` command run on a transit node

---
Table 44-2: Example output from the `show epsr` command run on a master node

<table>
<thead>
<tr>
<th>EPSR Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name ................... test4</td>
</tr>
<tr>
<td>Mode ..................... Master</td>
</tr>
<tr>
<td>Status .................... Enabled</td>
</tr>
<tr>
<td>State .................... Complete</td>
</tr>
<tr>
<td>Control Vlan ............ 4</td>
</tr>
<tr>
<td>Data VLAN(s) ............ 20</td>
</tr>
<tr>
<td>Interface Mode .......... Ports Only</td>
</tr>
<tr>
<td>Primary Port ............. port1.0.3</td>
</tr>
<tr>
<td>Primary Port Status ...... Forwarding</td>
</tr>
<tr>
<td>Secondary Port ........... port1.0.4</td>
</tr>
<tr>
<td>Secondary Port Status ... Forwarding</td>
</tr>
<tr>
<td>Hello Time ............... 1 s</td>
</tr>
<tr>
<td>Failover Time ............ 2 s</td>
</tr>
<tr>
<td>Ring Flap Time ........... 0 s</td>
</tr>
<tr>
<td>Trap ........................ Enabled</td>
</tr>
<tr>
<td>Enhanced Recovery ........ Disabled</td>
</tr>
</tbody>
</table>

**NOTE:** The above screen is only viewable when running the switch as an EPSR Master.

Running the switch as a master requires a Premium license.

Output: superloop topology

The following examples show the output display for superloop topology network.

Table 44-3: Example output from the `show epsr` command run on a Master Node

<table>
<thead>
<tr>
<th>EPSR Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name ................... test4</td>
</tr>
<tr>
<td>Mode ..................... Master</td>
</tr>
<tr>
<td>Status .................... Enabled</td>
</tr>
<tr>
<td>State .................... Complete</td>
</tr>
<tr>
<td>Control Vlan ............ 4</td>
</tr>
<tr>
<td>Data VLAN(s) ............ 20</td>
</tr>
<tr>
<td>Interface Mode .......... Ports Only</td>
</tr>
<tr>
<td>Primary Port ............. port1.0.3</td>
</tr>
<tr>
<td>Status .................... Forwarding (logically blocking)</td>
</tr>
<tr>
<td>Is On Common Segment ..... No</td>
</tr>
<tr>
<td>Blocking Control .......... Physical</td>
</tr>
<tr>
<td>Secondary Port ........... port1.0.4</td>
</tr>
<tr>
<td>Status .................... Blocked</td>
</tr>
<tr>
<td>Is On Common Segment ..... No</td>
</tr>
<tr>
<td>Blocking Control .......... Physical</td>
</tr>
<tr>
<td>Hello Time ............... 1 s</td>
</tr>
<tr>
<td>Failover Time ............ 2 s</td>
</tr>
<tr>
<td>Ring Flap Time ........... 0 s</td>
</tr>
<tr>
<td>Trap ........................ Enabled</td>
</tr>
<tr>
<td>Enhanced Recovery ........ Disabled</td>
</tr>
<tr>
<td>SLP Priority ............. 12</td>
</tr>
</tbody>
</table>
NOTE:
The above screen is only viewable when running the switch as an EPSR Master.
Running the switch as a master requires a Premium license.

Table 44-4: Example output from the *show epsr* command run on a Transit Node

<table>
<thead>
<tr>
<th>EPSR Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Mode</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>State</td>
</tr>
<tr>
<td>Control Vlan</td>
</tr>
<tr>
<td>Data VLAN(s)</td>
</tr>
<tr>
<td>Interface Mode</td>
</tr>
<tr>
<td>Primary Port</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Is On Common Segment</td>
</tr>
<tr>
<td>Blocking Control</td>
</tr>
<tr>
<td>Secondary Port</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Is On Common Segment</td>
</tr>
<tr>
<td>Blocking Control</td>
</tr>
<tr>
<td>Hello Time</td>
</tr>
<tr>
<td>Failover Time</td>
</tr>
<tr>
<td>Ring Flap Time</td>
</tr>
<tr>
<td>Trap</td>
</tr>
<tr>
<td>Enhanced Recovery</td>
</tr>
<tr>
<td>SLP Priority</td>
</tr>
</tbody>
</table>

Table 44-5: Parameters displayed in the output of the *show epsr* command

<table>
<thead>
<tr>
<th>Parameter on Master Node</th>
<th>Parameter on Transit Node</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name</td>
<td>The name of the EPSR instance.</td>
</tr>
<tr>
<td>Mode</td>
<td>Mode</td>
<td>The mode in which the EPSR instance is configured - either Master or Transit</td>
</tr>
<tr>
<td>Status</td>
<td>Status</td>
<td>Indicates whether the EPSR instance is enabled or disabled</td>
</tr>
<tr>
<td>State</td>
<td>State</td>
<td>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.</td>
</tr>
<tr>
<td>Control Vlan</td>
<td>Control Vlan</td>
<td>Displays the VID of the EPSR instance's control VLAN.</td>
</tr>
<tr>
<td>Data VLAN(s)</td>
<td>Data VLAN(s)</td>
<td>The VID(s) of the instance's data VLANs.</td>
</tr>
<tr>
<td>Interface Mode</td>
<td>Interface Mode</td>
<td>Whether the EPSR instance's ring ports are both physical ports (Ports Only) or are both static aggregators (Channel Groups Only).</td>
</tr>
<tr>
<td>Primary Port</td>
<td>First Port</td>
<td>The EPSR instance's primary ring port.</td>
</tr>
</tbody>
</table>
### EPSR COMMANDS

#### SHOW EPSR

**Table 44-5: Parameters displayed in the output of the `show epsr` command (cont.)**

<table>
<thead>
<tr>
<th>Parameter on Master Node</th>
<th>Parameter on Transit Node</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Status</td>
<td>- Status</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Direction</td>
<td>The ring port on which the last EPSR control packet was received is indicated by “Upstream”. The other ring port is then “Downstream”</td>
</tr>
<tr>
<td>- Is On Common Segment</td>
<td>- Is On Common Segment</td>
<td>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.</td>
</tr>
<tr>
<td>- Blocking Control</td>
<td>- Blocking Control</td>
<td>Whether the instance has “physical” or “logical” control of the ring port’s blocking in the instance’s data VLANs.</td>
</tr>
<tr>
<td>Secondary Port</td>
<td>Second Port</td>
<td>The EPSR instance’s secondary port.</td>
</tr>
<tr>
<td>- Status</td>
<td>- Status</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Direction</td>
<td>The ring port on which the last EPSR control packet was received is indicated by “Upstream”. The other ring port is then “Downstream”</td>
</tr>
<tr>
<td>- Is On Common Segment</td>
<td>- Is On Common Segment</td>
<td>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.</td>
</tr>
<tr>
<td>- Blocking Control</td>
<td>- Blocking Control</td>
<td>Whether the instance has “physical” or “logical” control of the ring port’s blocking in the instance’s data VLANs.</td>
</tr>
<tr>
<td>Hello Time</td>
<td></td>
<td>The EPSR instance’s setting for the interval between transmissions of health check messages (in seconds)</td>
</tr>
<tr>
<td>Failover Time</td>
<td></td>
<td>The time (in seconds) the EPSR instance waits to receive a health check message before it decides the ring is down</td>
</tr>
<tr>
<td>Ring Flap Time</td>
<td></td>
<td>The minimum time the EPSR instance must remain in the failed state</td>
</tr>
<tr>
<td>Trap</td>
<td>Trap</td>
<td>Whether the EPSR instance has EPSR SNMP traps enabled</td>
</tr>
</tbody>
</table>
Table 44-5: Parameters displayed in the output of the `show epsr` command (cont.)

<table>
<thead>
<tr>
<th>Parameter on Master Node</th>
<th>Parameter on Transit Node</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced Recovery</td>
<td>Enhanced Recovery</td>
<td>Whether the EPSR instance has enhanced recovery mode enabled</td>
</tr>
<tr>
<td>SLP Priority</td>
<td>SLP Priority</td>
<td>The EPSR instance’s priority (for SuperLoop Prevention)</td>
</tr>
</tbody>
</table>

**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 44-6: Example output from the `show epsr common segments` command

<table>
<thead>
<tr>
<th>EPSR Common Segments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Seg</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>port1.0.24</td>
</tr>
<tr>
<td>test_inst_Blue</td>
</tr>
<tr>
<td>test_inst_Green</td>
</tr>
<tr>
<td>sa4</td>
</tr>
<tr>
<td>testB</td>
</tr>
<tr>
<td>sa5</td>
</tr>
<tr>
<td>test_77</td>
</tr>
</tbody>
</table>

**Related Commands**
- show epsr
- show epsr summary
- show epsr counters
show epsr config-check

**Overview**  This command checks the configuration of a specified EPSR instance, or all EPSR instances.

If an instance is enabled, this command will check for the following errors or warnings:

- The control VLAN has the wrong number of ports.
- There are no data VLANs.
- Some of the data VLANs are not assigned to the ring ports.
- The failover time is less than 5 seconds, for a stacked device.
- The instance is a master that shares a common segment with a higher priority instance.
- The instance is a master that shares a common segment with another master.
- The instance is a master with its secondary port on a common segment.

**Syntax**  show epsr [instance] config-check

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance</td>
<td>Name of the EPSR instance to check on.</td>
</tr>
</tbody>
</table>

**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 44-7: Example output from the show epsr config-check command**

<table>
<thead>
<tr>
<th>EPSR Instance</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>red</td>
<td>Warning</td>
<td>Failover time is 2s but should be 5s because device is stacked.</td>
</tr>
<tr>
<td>white</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>blue</td>
<td>Warning</td>
<td>Primary port is not in data VLANs 29-99.</td>
</tr>
<tr>
<td>orange</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>

Don't forget to check that this node's configuration is consistent with all other nodes in the ring.
EPSR COMMANDS
SHOW EPSR CONFIG-CHECK

**Related Commands**

*show epsr*
show epsr <epsr-instance>

**Overview**  This command displays information about the specified EPSR instance.

**Syntax**  show epsr <epsr-instance>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;epsr-instance&gt;</td>
<td>Name of the EPSR instance.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example**  To show the current settings of the EPSR instance called blue, use the command:

```bash
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**
```bash
show epsr <epsr-instance> counters
```

**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 44-8: Example output from the show epsr summary command

<table>
<thead>
<tr>
<th>EPSR Summary Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviations:</td>
</tr>
<tr>
<td>M = Master node</td>
</tr>
<tr>
<td>T = Transit node</td>
</tr>
<tr>
<td>C = is on a common segment with other instances</td>
</tr>
<tr>
<td>P = instance on a common segment has physical control of the shared port’s data VLAN blocking</td>
</tr>
<tr>
<td>LB = ring port is Logically Blocking - applicable to master only</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EPSR Instance</th>
<th>Mode</th>
<th>Status</th>
<th>State</th>
<th>VLAN</th>
<th>Prio</th>
<th>Port Status</th>
<th>Port Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>test-12345</td>
<td>T</td>
<td>Enabled</td>
<td>Links-Down</td>
<td>6</td>
<td>127</td>
<td>Blocking (C,P)</td>
<td>Blocking (C,P)</td>
</tr>
<tr>
<td>test1</td>
<td>M</td>
<td>Enabled</td>
<td>Complete</td>
<td>5</td>
<td>12</td>
<td>Fwding</td>
<td>Fwding (LB)</td>
</tr>
<tr>
<td>test2</td>
<td>T</td>
<td>Enabled</td>
<td>Pre-Fwding</td>
<td>4</td>
<td>126</td>
<td>Fwding (C)</td>
<td>Blocking (C)</td>
</tr>
<tr>
<td>localB</td>
<td>T</td>
<td>Disabled</td>
<td>Idle</td>
<td>40</td>
<td>0</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>localC</td>
<td>T</td>
<td>Disabled</td>
<td>Idle</td>
<td>41</td>
<td>0</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
**Overview**  This command applies the functionality of the no variant of the `debug epsr` command.
Introduction

This chapter provides an alphabetical reference for AMF commands.

**AMF Naming Convention**

When AMF is enabled on a device, it will automatically be assigned a host name. If a host name has already been assigned, by using the command `hostname` on page 237, this will remain. If however, no host name has been assigned, then the name applied will be the prefix, `host_` followed (without a space) by the MAC address of the device. For example, a device whose MAC address is `0016.76b1.7a5e` will have the name `host_0016_76b1_7a5e` assigned to it.

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

Command List

- “atmf area” on page 1879
- “atmf area password” on page 1880
- “atmf backup” on page 1882
- “atmf backup area-masters delete” on page 1883
- “atmf backup area-masters enable” on page 1884
- “atmf backup area-masters now” on page 1885
- “atmf backup area-masters synchronize” on page 1886
- “atmf backup bandwidth” on page 1887
- “atmf backup delete” on page 1888
- “atmf backup enable” on page 1889
- “atmf backup now” on page 1890
- “atmf backup server” on page 1892
- “atmf backup stop” on page 1894
- “atmf backup synchronize” on page 1895
- “atmf cleanup” on page 1896
- “atmf controller” on page 1897
- “atmf distribute firmware” on page 1898
- “atmf domain vlan” on page 1900
- “atmf enable” on page 1902
- “atmf group (membership)” on page 1903
- “atmf log-verbose” on page 1905
- “atmf management subnet” on page 1906
- “atmf management vlan” on page 1908
- “atmf master” on page 1910
- “atmf network-name” on page 1911
- “atmf provision” on page 1912
- “atmf provision node clone” on page 1913
- “atmf provision node configure boot config” on page 1915
- “atmf provision node configure boot system” on page 1917
- “atmf provision node create” on page 1919
- “atmf provision node delete” on page 1921
- “atmf provision node license-cert” on page 1923
- “atmf provision node locate” on page 1925
- “atmf reboot-rolling” on page 1926
- “atmf recover” on page 1930
AMF COMMANDS

- “atmf recover led-off” on page 1932
- “atmf remote-login” on page 1933
- “atmf restricted-login” on page 1934
- “atmf select-area” on page 1935
- “atmf virtual-link” on page 1936
- “atmf working-set” on page 1939
- “clear atmf links statistics” on page 1941
- “debug atmf” on page 1942
- “debug atmf packet” on page 1944
- “erase factory-default” on page 1947
- “show atmf” on page 1948
- “show atmf area” on page 1952
- “show atmf area summary” on page 1955
- “show atmf area nodes” on page 1956
- “show atmf area nodes-detail” on page 1958
- “show atmf backup” on page 1960
- “show atmf backup area” on page 1963
- “show atmf detail” on page 1965
- “show atmf group” on page 1967
- “show atmf group members” on page 1969
- “show atmf links” on page 1971
- “show atmf links detail” on page 1972
- “show atmf links statistics” on page 1981
- “show atmf memory” on page 1986
- “show atmf nodes” on page 1988
- “show atmf provision nodes” on page 1989
- “show atmf tech” on page 1990
- “show atmf working-set” on page 1993
- “show debugging atmf” on page 1994
- “show debugging atmf packet” on page 1995
- “show running-config atmf” on page 1996
- “switchport atmf-arealink remote-area” on page 1997
- “switchport atmf-crosslink” on page 1998
- “switchport atmf-link” on page 2000
- “type atmf node” on page 2001
• “undebug atmf” on page 2004
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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;area-name&gt;</code></td>
<td>The AMF area name. Up to 15 printable characters can be entered for the name. Names are case sensitive and must be unique within an AMF network.</td>
</tr>
<tr>
<td><code>&lt;1-126&gt;</code></td>
<td>An ID number that uniquely identifies this area.</td>
</tr>
<tr>
<td><code>local</code></td>
<td>Set the area to be the local area. The local area contains the device you are configuring.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Usage**
This command enables you to divide your AMF network into areas. Each area is managed by at least one master node. Each area can have up to 120 nodes, depending on the license installed on that area's master node.

The whole AMF network is managed by up to 8 AMF controllers. Each AMF controller can communicate with multiple areas. The number of areas supported on a controller depends on the license installed on that controller.

You must give each area in an AMF network a unique name and ID number.

Only one local area can be configured on a device. You must specify a local area on each controller, remote AMF master, and gateway node.

**Example**
To create the AMF area named *New-Zealand*, with an ID of 1, and specify that it is the local area, use the command:
```
controller-1(config)# atmf area New-Zealand id 1 local
```
To configure a remote area named *Auckland*, with an ID of 100, use the command:
```
controller-1(config)# atmf area Auckland id 100
```

**Related Commands**
atmf area password
show atmf area
show atmf area summary
show atmf area nodes
switchport atmf-arealink remote-area
### AMF Commands

#### 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**

```plaintext
atmf area <area-name> password [8] <password>
no atmf area <area-name> password
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;area-name&gt;</code></td>
<td>The AMF area name.</td>
</tr>
<tr>
<td><code>8</code></td>
<td>This parameter is displayed in <code>show running-config</code> output to indicate that it is displaying the password in encrypted form. You should not enter <code>8</code> on the CLI yourself.</td>
</tr>
<tr>
<td><code>&lt;password&gt;</code></td>
<td>The password is between 8 and 32 characters long. It can include spaces.</td>
</tr>
</tbody>
</table>

**Mode**

Global Configuration

**Usage**

You must configure a password on each area that an AMF controller communicates with, except for the controller’s local area. The areas must already have been created using the `atmf area` command.

Enter the password identically on both of:

- the area that locally contains the controller, and
- the remote area

The command `show running-config atmf` will display the encrypted version of this password. The encryption keys will match between the controller and the remote AMF master.

If multiple controller and masters exist in an area, they must all have the same area configuration.

**Example**

To give the AMF area named *Auckland* a password of “secure#1” use the following command on the controller:

```plaintext
controller-1(config)# atmf area Auckland password secure#1
```

and also use the following command on the master node for the Auckland area:

```plaintext
auck-master(config)# atmf area Auckland password secure#1
```
AMF COMMANDS

ATMF AREA PASSWORD

Related Commands

atmf area
show atmf area
show atmf area summary
show atmf area nodes
switchport atmf-arealink remote-area
atmf backup

**Overview**  This command can only be applied to a master node. It manually schedules an AMF backup to start at a specified time and to execute a specified number of times per day.

Use the **no** variant of this command to disable the schedule.

**Syntax**  

```
atmf backup {default|<hh:mm> frequency <1-24>}
no atmf backup enable
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Restore the default backup schedule.</td>
</tr>
<tr>
<td><a href="">hh:mm</a></td>
<td>Sets the time of day to apply the first backup, in hours and minutes. Note that this parameter uses the 24 hour clock.</td>
</tr>
<tr>
<td>backup</td>
<td>Enables AMF backup to external media.</td>
</tr>
<tr>
<td>frequency &lt;1-24&gt;</td>
<td>Sets the number of times within a 24 hour period that backups will be taken.</td>
</tr>
</tbody>
</table>

**Default**  Backups run daily at 03:00 AM, by default

**Mode**  Global Configuration

**Usage**  Running this command only configures the schedule. To enable the schedule, you should then apply the command **atmf backup enable**.

**Example**  To schedule backup requests to begin at 11 am and execute twice per day (11 am and 11 pm), use the following command:

```
node_1# configure terminal
node_1(config)# atmf backup 11:00 frequency 2
```

**CAUTION:** File names that comprise identical text, but with differing case, such as Test.txt and test.txt, will not be recognized as being different on a FAT32 based backup media such as a USB storage device. However, these filenames will be recognized as being different on your Linux based device. Therefore, for good practice, ensure that you apply a consistent case structure for your back-up file names.

**Related Commands**  

- atmf backup enable
- atmf backup stop
- show atmf backup
atmf backup area-masters delete

**Overview**
Use this command to delete a backup of a specified node in a specified area. This command is only valid on AMF controllers.

**Syntax**
```atmf backup area-masters delete area <area-name> node <node-name>```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-name&gt;</td>
<td>The area that contains the node whose backup will be deleted.</td>
</tr>
<tr>
<td>&lt;node-name&gt;</td>
<td>The node whose backup will be deleted.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
To delete the backup of the remote area-master named “well-gate” in the area Wellington, use the command:

```controller-1# atmf backup area-masters delete area Wellington node well-gate```

**Related Commands**
show atmf backup area
**Overview**
Use this command to enable backup of remote area-masters from the AMF controller. This command is only valid on AMF controllers.

Use the **no** form of the command to stop backups of remote area-masters.

**Syntax**
```
atmf backup area-masters enable
no atmf backup area-masters enable
```

**Mode**
Global configuration

**Default**
Remote area backups are disabled by default

**Usage**
Use the following commands to configure the remote area-master backups:
- `atmf backup` to configure when the backups begin and how often they run
- `atmf backup server` to configure the backup server.

**Example**
To enable scheduled backups of AMF remote area-masters, use the commands:
```
controller-1# configure terminal
controller-1(config)# atmf backup area-masters enable
```

To disable scheduled backups of AMF remote area-masters, use the commands:
```
controller-1# configure terminal
controller-1(config)# no atmf backup area-masters enable
```

**Related Commands**
- `atmf backup server`
- `atmf backup`
- `show atmf backup area`
**atmf backup area-masters now**

**Overview**  
Use this command to run a backup of one or more remote area-masters from the AMF controller immediately. This command is only valid on AMF controllers.

**Syntax**  
```
atmf backup area-masters now [area <area-name>|area <area-name> node <node-name>]
```

**Mode**  
Privileged Exec

**Example**  
To back up all local master nodes in all areas controlled by controller-1, use the command
```
controller-1# atmf backup area-masters now
```
To back up all local masters in the Wellington area, use the command
```
controller-1# atmf backup area-masters now area Wellington
```
To back up the local master “well-master” in the Wellington area, use the command
```
controller-1# atmf backup area-masters now area Wellington node well-master
```

**Related Commands**  
- atmf backup area-masters enable
- atmf backup area-masters synchronize
- show atmf backup area
**Overview**  
Use this command to synchronise backed-up area-master files between the active remote file server and the backup remote file server. Files are copied from the active server to the remote server.

This command is only valid on AMF controllers.

**Syntax**  
`atmf backup area-masters synchronize`

**Mode**  
Privileged Exec

**Example**  
To synchronize backed-up files between the remote file servers for all area-masters, use the command:

```
controller-1# atmf backup area-masters synchronize
```

**Related Commands**  
- `atmf backup area-masters enable`
- `atmf backup area-masters now`
- `show atmf backup area`
ATMF BACKUP BANDWIDTH

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
```

**Default**  
The default value is zero, allowing unlimited bandwidth when executing an AMF backup.

**Mode**  
Global Configuration

**Examples**

To set an `atmf backup bandwidth` of 750 kBps, use the commands:

```
node2# configure terminal
node2(config)# atmf backup bandwidth 750
```

To set the AMF backup bandwidth to the default value for unlimited bandwidth, use the commands:

```
node2# configure terminal
node2(config)# no atmf backup bandwidth
```

**Related Commands**

`show atmf backup`
atmf backup delete

**Overview**  This command removes the backup file from the external media of a specified AMF node.

**Syntax**  atmf backup delete <node-name>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;node-name&gt;</td>
<td>The AMF node name of the backup file to be deleted.</td>
</tr>
</tbody>
</table>
atmf backup enable

**Overview**  This command enables automatic AMF backups on the AMF master node that you are connected to. By default, automatic backup starts at 3:00 AM. However, this schedule can be changed by the `atmf backup` command. Note that backups are initiated and stored only on the master nodes.

Use the `no` variant of this command to disable any AMF backups that have been scheduled and previously enabled.

**Syntax**
```
atmf backup enable
no atmf backup enable
```

**Default**  Automatic AMF backup functionality is enabled on the AMF master when it is configured and external media, i.e. an SD card or a USB storage device or remote server, is detected.

**Mode**  Global Configuration

**Usage**  A warning message will appear if you run the `atmf backup enable` command with either insufficient or marginal memory availability on your external storage device.

You can use the command `show atmf backup` on page 1960 to check the amount of space available on your external storage device.

**Example**  To turn on automatic AMF backup, use the following command:
```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup enable
```

**Related Commands**
- `show atmf`
- `show atmf backup`
- `atmf backup`
- `atmf backup now`
- `atmf enable`
atmf backup now

**Overview**  This command initiates an immediate AMF backup of either all AMF members, or a selected AMF member. Note that this backup information is stored in the external media on the master node of the device on which this command is run, even though the selected AMF member may not be a master node.

**Syntax**  
```
 atmf backup now [ <nodename> ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;nodename&gt; or &lt;hostname&gt;</td>
<td>The name of the AMF member to be backed up, as set by the command hostname on page 237. 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.</td>
</tr>
</tbody>
</table>

**Default**  A backup is initiated for all nodes on the AMF (but stored on the master nodes).

**Mode**  Privileged Exec

**Usage**  Although this command will select the AMF node to be backed-up, it can only be run from any AMF master node.

*NOTE:* The backup produced will be for the selected node but the backed-up config will reside on the external media of the AMF master node on which the command was run. However, this process will result in the information on one master being more up-to-date. To maintain concurrent backups on both masters, you can apply the backup now command to the master working-set. This is shown in Example 4 below.

**Example 1**  In this example, an AMF member has not been assigned a host name. The following command is run on the AMF_Master_2 node to immediately backup the device that is identified by its MAC address of 0016.76b1.7a5e:

```
AMF_Master_2# atmf backup now host_0016_76b1_7a5e
```

*NOTE:* When a host name is derived from its MAC address, the syntax format entered changes from XXXX.XXXX.XXXX to XXXX.XXXX.XXXX.

**Example 2**  In this example, an AMF member has the host name, *office_annex*. The following command will immediately backup this device:

```
AMF_Master_2# atmf backup now office_annex
```

This command is initiated on the device’s master node named *AMF_Master_2* and initiates an immediate backup on the device named *office_annex*.

**Example 3**  To initiate from AMF_master_1 an immediate backup of all AMF member nodes, use the following command:

```
AMF_Master_1# amf backup now
```
**Example 4** To initiate an immediate backup of the node with the host-name "office_annex" and store the configuration on both masters, use the following process:

From the AMF_master_1, set the working-set to comprise only of the automatic group, master nodes.

```
AMF_Master_1# atmf working-set group master
```

This command returns the following display:

```
--------------------------------
AMF_Master_1, AMF_Master_2
--------------------------------
Working set join
```

Backup the AMF member with the host name, **office_annex** on both the master nodes as defined by the working set.

```
AMF_Master[2]# atmf backup now office_annex
```

Note that the [2] shown in the command prompt indicates a 2 node working-set.

**Related Commands**

- **atmf backup**
- **atmf backup stop**
- **hostname**
- **show atmf backup**
**atmf backup server**

**Overview**  
This command configures remote file servers as the destination for AMF backups. Use the `no` variant of this command to remove the destination server(s). When all servers are removed the system will revert to backup from external media.

**Syntax**  
```
atmf backup server id {1|2} <hostlocation> username <username> [path <path>|port <1-65535>]
```
```
o atmf backup server id {1|2}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Remote server backup server identifier.</td>
</tr>
<tr>
<td>(1</td>
<td>2)</td>
</tr>
<tr>
<td>&lt;hostlocation&gt;</td>
<td>Either the name or the IP address (IPv4 or IPv6) of the selected backup server (1 or 2).</td>
</tr>
<tr>
<td>username</td>
<td>Configure the username to log in with on the selected remote file server.</td>
</tr>
<tr>
<td>&lt;username&gt;</td>
<td>The selected remote file server's username.</td>
</tr>
<tr>
<td>path</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;path&gt;</td>
<td>The directory path utilized to store the backup files on the selected remote file server. No spaces are allowed in the path.</td>
</tr>
<tr>
<td>port</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>A TCP port within the specified range.</td>
</tr>
</tbody>
</table>

**Defaults**  
Remote backup servers are not configured. The default SSH TCP port is 22. The path utilized on the remote file server is the home directory of the username.

**Mode**  
Global Exec

**Usage**  
The hostname and username parameters must both be configured.

**Examples**  
To configure server 1 with an IPv4 address and a username of `backup1`, use the commands:

```plaintext
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`
AMF Commands
ATMF BACKUP STOP

atmf backup stop

Overview  Running this command stops a backup that is currently running on the master node you are logged onto. Note that if you have two masters and want to stop both, then you can either run this command separately on each master node, or add both masters to a working set, and issue this command to the working set.

Syntax  atmf backup stop

Mode  Privileged Exec

Usage  This command is used to halt an AMF backup that is in progress. In this situation the backup process will finish on its current node and then stop.

Example  To stop a backup that is currently executing on master node node-1, use the following command:

   AMF_Master_1# amf backup stop

Related Commands  atmf backup
                 atmf backup enable
                 atmf backup now
                 show atmf backup
**Overview**
For the master node you are connected to, this command initiates a system backup of files from the node’s active remote file server to its backup remote file server. Note that this process happens automatically each time the network is backed up.

**Syntax**
```
atmf backup synchronize
```

**Mode**
Privileged Exec

**Example**
When connected to the master node AMF_Master_1, the following command will initiate a backup of all system related files from its active remote file server to its backup remote file server.

```
AMF_Master_1# atmf backup synchronize
```

**Related Commands**
- `show atmf backup`
- `atmf backup enable`
- `show atmf`
**Overview**  This command erases all data from NVS and all data from Flash **excluding** the following:

- The current release file and its `/flash/.release` file
- The backup release file and `/flash/.backup` file
- v1 license files `/flash/.configs/.swfeature.lic`
- v2 license files `/flash/.configs/.sw_v2.lic`

It then reboots to put the device in a clean state ready to be used as a replacement node on a provisioned port.

**Syntax**  `atmf cleanup`

**Mode**  Privileged Exec

**Usage**  This command is an alias to the `erase factory-default` command.

**Example**  To erase data, use the command:

```
Node_1# atmf cleanup
```

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

**Related Commands**  `erase factory-default`
atmf controller

**Overview**
Use this command to configure the device as an AMF controller. This enables you to split a large AMF network into multiple areas.

The number of areas supported on a controller depends on the license installed on that controller.

**Syntax**
```
atmf controller
no atmf controller
```

**Mode**
Global configuration

**Usage**
A valid AMF license must be available before this command can be applied.

**Example**
To configure the node named `controller-1` as an AMF controller, use the commands:
```
controller-1# configure terminal
controller-1(config)# atmf controller
```

To stop the node named `controller-1` from being an AMF controller, use the commands:
```
controller-1# configure terminal
controller-1(config)# no atmf controller
```

**Related Commands**
```
atmf area
show atmf
```
atmf distribute firmware

**Overview**  This command can be used to upgrade software one AMF node at a time. A URL can be selected from any media location. The latest compatible release for a node will be selected from this location.

Several procedures are performed to ensure the upgrade will succeed. This includes checking the current node release boots from flash. If there is enough space on flash the software release is copied to flash on the new location.

The new release name is updated using the `boot system` command. The old release will become the backup release file. If a release file exists in a remote device (such as TFTP or HTTP, for example) then the URL should specify the exact release filename without using a wild card character.

The command will continue to upgrade software until all nodes are upgraded. At the end of the upgrade cycle the `reboot` command should be used on the working-set.

**Syntax**  `atmf distribute firmware <filename>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filename&gt;</code></td>
<td>The filename and path of the file. See the File Management Feature Overview and Configuration Guide for valid syntax.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Examples**  To upgrade nodes in a AMF network with a predefined AMF group called `sw_team`, use the following commands:

```
SW_Team1# atmf working-set group sw_team
```

**Output**

```
ATMF_NETWORK[3]# atmf distribute firmware card:*.rel
```

---

1898  Command Reference for x510 Series Switches  C613-50058-01 REV A

AlliedWare Plus™ Operating System - Version 5.4.5-0.x
### Output

Retrieving data from SW_Team1
Retrieving data from SW_Team2
Retrieving data from SW_Team3

ATMF Firmware Upgrade:

<table>
<thead>
<tr>
<th>Node Name</th>
<th>New Release File</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW_Team1</td>
<td>x510-main-20140204-2.rel</td>
<td>Release ready</td>
</tr>
<tr>
<td>SW_Team2</td>
<td>x610-main-20140204-2.rel</td>
<td>Release ready</td>
</tr>
<tr>
<td>SW_Team3</td>
<td>x610-main-20140204-2.rel</td>
<td>Release ready</td>
</tr>
</tbody>
</table>

Continue the rolling reboot? (y/n): y

Copying Release : x510-main-20140204-2.rel to SW_Team1
Updating Release : x510-main-20140204-2.rel information on SW_Team1

Copying Release : x610-main-20140204-2.rel to SW_Team2
Updating Release : x610-main-20140204-2.rel information on SW_Team2

Copying Release : x610-main-20140204-2.rel to SW_Team3
Updating Release : x610-main-20140204-2.rel information on SW_Team3

New firmware will not take effect until nodes are rebooted.

ATMF_NETWORK[3]#
atmf domain vlan

**Overview**  The AMF domain vlan is one of the internal VLANs that are used to communicate information about the state of the AMF network between nodes. AMF uses its internal VLANS (the management VLAN and the domain VLAN) to communicate its inter nodal network status information. These VLANs must be reserved for AMF and not used for other purposes.

When an AMF network is first created all its nodes are assigned a domain VLAN with a default (domain) VID of 4091. An important point conceptually is that although this VLAN then exists globally across the AMF network, it is assigned separately to each domain. The AMF network therefore can be thought of as comprising a series of domain VLANS each having the same VID and each being applied to a horizontal slice (domain) of the AMF. It follows therefore that the domain VLANS are only applied to ports that form cross-links and not to ports that form uplinks/downlinks.

If you assign a VLAN ID to this VLAN (i.e. changing its value from the default of 4091) then you will need to do this separately on every device within the AMF network. The AMF domain subnet will then be applied to this new VID when all devices within the AMF network are next rebooted.

Use the **no** variant of this command to reset the VLAN ID to its default value of 4091.

**Syntax**
```
 atmf domain vlan <2-4090>
 no atmf domain_vlan
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;2-4090&gt;</td>
<td>The VLAN number in the range 2 to 4090.</td>
</tr>
</tbody>
</table>

**Default**  The default domain VLAN ID for the AMF is 4091.

**Mode**  Global Configuration

**Usage**  The VLANs involved in this process must be reserved for AMF and cannot be used for other purposes. This command enables you to change the domain VLAN to match your network's specific configuration.

**CAUTION:** Setting this command, then rebooting the device, will only apply the AMF VLAN for the device being configured. The new domain VLAN will not become effective for the AMF network until all its member nodes have been updated, and all its member devices rebooted.

As part of its automatic creation process, this VLAN will also be assigned an IP subnet address based on the value configured by the command **atmf management subnet** on page 1906. Refer to this command for more information.
Examples

To change the AMF domain VLAN to 4000 use the following commands:

```
node-1# configure terminal
node-1(config)# atmf domain vlan 4000
```

To reset the AMF domain VLAN to its default of 4091, use the following commands:

```
node-1# configure terminal
node-1(config)# no atmf domain vlan
```
### Overview
This command manually enables (turns on) the AMF feature for the device being configured.

**Use the no variant of this command to disable (turn off) the AMF feature on the member node.**

### Syntax
```
atmf enable
no atmf enable
```

### Default
Once AMF is configured, the AMF feature starts automatically when the device starts up.

### Mode
Global Configuration

### Usage
The device does not auto negotiate AMF domain specific settings such as the Network Name. You should therefore, configure your device with any domain specific (non default) settings before enabling AMF.

### Examples
To turn off AMF, use the command:
```
MyNode# config terminal
MyNode(config)# no atmf enable
```

To turn on AMF, use the command:
```
MyNode(config)# atmf enable
```

This command returns the following display:

```
% Warning: The ATMF network config has been set to enable
% Save the config and restart the system for this change to take effect.
```
Overview
This command configures a device to be a member of one or more AMF groups. Groups exist in three forms: Implicit Groups, Automatic Groups, and User-defined Groups.

- Implicit Groups
  - all: All nodes in the AMF
  - current: The current working-set
  - local: The originating node.

Note that the Implicit Groups do not appear in show group output.

- Automatic Groups - These are defined by hardware architecture, e.g. x510, x610, x8100, AR3050S, AR4050S.

- User-defined Groups - These enable you to define arbitrary groups of AMF members based on your own criteria.

Each node in the AMF is automatically assigned membership to the implicit groups, and the automatic groups that are appropriate to its node type, e.g. x610, PoE. Similarly, nodes that are configured as masters are automatically assigned to the master group.

Use the no variant of this command to remove the membership.

Syntax
```
atmf group <group-list>
natmf group <group-list>
```

Mode
Global Configuration

Usage
You can use this command to define your own arbitrary groups of AMF members based on your own network's configuration requirements. Applying a node to a non-existing group will result in the group automatically being created.

Note that the master nodes are automatically assigned to be members of the pre-existing master group.

The following example configures the device to be members of three groups; two are company departments, and one comprises all devices located in building_2. To avoid having to run this command separately on each device that is to be added to these groups, you can remotely assign all of these devices to a working-set, then use the capabilities of the working-set to apply the `atmf group (membership)` command to all members of the working set.
Example 1  To specify the device to become a member of AMF groups named marketing, sales, and building_2, use the following commands:

node-1# configure terminal
node-1(config)# atmf group marketing,sales,building_2

Example 2  To add the nodes member_node_1 and member_node_2 to groups building1 and sales, first add the nodes to the working-set:

master_node# atmf working-set member_node_1,member_node_2

This command returns the following output confirming that the nodes member_node_1 and member_node_2 are now part of the working-set:

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.

AMF group information
building1, sales

Related Commands
show atmf group
show atmf group members
atmf log-verbose

**Overview**
This command limits the number of log messages displayed on the console or permanently logged.

**Syntax**

```
atmf log-verbose <1-3>
no atmf log-verbose
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-3&gt;</td>
<td>The verbose limitation (3 = noisiest, 1 = quietest)</td>
</tr>
</tbody>
</table>

**Default**
The default log display is 3.

**Usage**
This command is intended for use in large networks where verbose output can make the console unusable for periods of time while nodes are joining and leaving.

**Mode**
Global Configuration

**Example**
To set the log-verbose to noise level 2, use the command:
```
node-1# configure terminal
node-1(config)# atmf log-verbose 2
```

**Validation Command**
`show atmf`
**atmf management subnet**

**Overview**  
This command is used to assign a subnet that will be allocated to the AMF management and domain management VLANs. From the address space defined by this command, two subnets are created, a management subnet component and a domain component, as explained in the Usage section of this command description.

AMF uses these internal IPv4 subnets when exchanging its inter nodal status packets. These subnet addresses must be reserved for AMF and should be used for no other purpose.

The new management subnet will not become effective until all members of the AMF network have been updated and all its units rebooted.

Use the `no` variant of this command to remove the assigned subnet VLANs.

**Syntax**

atmf management subnet `<a.b.0.0>`

no atmf management subnet

**Parameter**

| `<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. Asubnet mask of 255.255.0.0 will automatically be applied.

**Mode**

Global Configuration

**Usage**

Typically a network administrator would use this command to change the default subnet address to match local network requirements.

As previously mentioned, running this command will result in the creation of a further two subnets (within the class B address space assigned) and the mask will extend from /16 to /17.

For example, if the management subnet is assigned the address 172.31.0.0/16, this will result in the automatic creation of the following two subnets:

- 172.31.0.0/17 assigned to the atmf management vlan
- 172.31.128.0/17 assigned to the atmf domain vlan.

**Examples**

To change the AMF management subnet address on node node-1 to 172.25.0.0:

```bash
node-1# configure terminal
node-1(config)# atmf management subnet 172.25.0.0
```
To change the AMF management subnet address on node node-1 back to its default of 172.31.0.0:

node-1# configure terminal
node-1(config)# no atmf management subnet
The AMF management VLAN is created when the AMF network is first initiated and is assigned its default VID of 4092. This command enables you to change the VID from this default value.

The AMF management VLAN is one of the internal VLANs that are used to communicate information about the state of the AMF network between nodes. AMF uses its internal VLANs (such as the management VLAN and the domain VLAN) to communicate its inter-nodal network status information. These VLANs must be reserved for AMF and not used for other purposes.

If you assign a VLAN ID to this VLAN (i.e. change its value from the default of 4092) then you will need to do this separately on every device within the AMF. The AMF management subnet will then be applied to this new VID when all devices within the AMF network are next rebooted.

Use the **novariant of this command to restore the VID to the default of 4092.**

### Syntax

```
atmf management vlan 2-4090>
```

```
no atmf management vlan
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-4090&gt;</td>
<td>The VID assigned to the AMF management VLAN.</td>
</tr>
</tbody>
</table>

### Default

The default VLAN ID for the AMF is 4092.

**NOTE:** Although the value applied by default lies outside the user configurable range. You can use the “no” form of this command to reset the VLAN to its default value.

### Mode

Global Configuration

### Usage

You can use this command to change the management VLAN to meet your network’s requirements and standards, particularly in situations where the default address value is unacceptable.

**NOTE:** This VLAN will automatically be assigned an IP subnet address based on the value configured by the command **atmf management subnet** on page 1906. Refer to this command description for further details.
Examples

To change the AMF management VLAN to 4090 use the following commands:

```
node-1# configure terminal
node-1(config)# atmf management vlan 4090
```

To reset the AMF domain VLAN to its default of 4092, use the following commands:

```
node-1# configure terminal
node-1(config)# no atmf management vlan
```

Related Commands

- `atmf domain vlan`
- `show atmf`
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`
AMF COMMANDS
ATMF NETWORK-NAME

atmf network-name

Overview  This command applies an AMF network name to a (prospective) AMF node. In order for an AMF network to be valid, its network-name must be configured on at least two nodes, one of which must be configured as a master and have an AMF License applied. These nodes may be connected using either AMF downlinks or crosslinks.

For more information on configuring an AMF master node, see atmf master. Use the no variant of this command to remove the AMF network name.

Syntax  atmf network-name <name>
        no atmf network-name

Mode  Global Configuration

Usage  This is one of the essential commands when configuring AMF and must be entered on each node that is to be part of the AMF. This command will not take effect until the particular node is rebooted.

A switching node (master or member) may be a member of only one AMF network.

CAUTION: Ensure that you enter the correct network name. Entering an incorrect name will cause the AMF network to fragment (at the next reboot).

Example  To set the AMF network name to amf_net use the command:

        Node_1(config)# atmf network-name amf_net

Parameter | Description
----------|------------------
<name>    | The AMF network name. Up to 15 printable characters can be entered for the network-name.
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;nodename&gt;</td>
<td>The name of the provisioned node that will appear on the AMF network in the future.</td>
</tr>
</tbody>
</table>

**Default**  No provision.

**Mode**  Interface Configuration

**Usage**  The port should be configured as an AMF link or cross link and should be “down” to add or remove a provisioned node.

**Example**  To provision an AMF node named node1 for port1.0.1, use the command:

```
host1(config)# interface port1.0.1
host1(config-if)# atmf provision node1
```

**Related Commands**

- switchport atmf-link
- switchport atmf-crosslink
- show atmf links
atmf provision node clone

**Overview**
This command sets up a space on the backup media for use with a provisioned node and copies into it almost all files and directories from a chosen backup or provisioned node.

Alternatively, you can set up a new, unique provisioned node by using the command `atmf provision node create`.

**Syntax**
```
atmf provision node <nodename> clone <source-nodename>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;nodename&gt;</code></td>
<td>The name that will be assigned to the clone when connected.</td>
</tr>
<tr>
<td><code>&lt;source-nodename&gt;</code></td>
<td>The name of the node whose configuration is to be copied for loading to the clone.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Usage**
This command is only available on master nodes in the AMF network.

You must run either this command or `atmf provision node create` command, before you can use other `atmf provision node` commands using the specified node name. If a backup or provisioned node already exists for the specified node then you must delete it before using the `atmf provision node clone` command.

When using this command it is important to be aware of the following:

- A copy of `<media>:atmf/<atmf_name>/nodes/<source_node>/flash` will be made for the provisioned node and stored in the backup media.
- The directory `<node_backup_dir>/flash/.config/ssh` is excluded from the copy.
- All contents of `<root_backup_dir>/nodes/<nodename>` will be deleted or overwritten.
- Settings for the expected location of other provisioned nodes are excluded from the copy.

The active and backup configuration files are automatically modified in the following ways:

- The `hostname` command is modified to match the name of the provisioned node.
- The `stack virtual-chassis-id` command is removed, if present.
### Example

To copy from the backup of device2 to create backup files for the new provisioned node device3 use the following command:

```
device1# atmf provision node device3 clone device2
```

Figure 45-1: Sample output from the **atmf provision node clone** command

```
device1#atmf provision node device3 clone device2
Copying...
Successful operation
```

To confirm that a new provisioned node has been cloned, use the command:

```
device1# show atmf backup
```

The output from this command is shown in the following figure, and shows the details of the new provisioned node device3.

Figure 45-2: Sample output from the **show atmf backup** command

```
device1#show atmf backup
Scheduled Backup ....... Enabled
  Schedule ............. 1 per day starting at 03:00
  Next Backup Time ..... 01 Jan 2014 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7297.0MB)
Server Config ..........
  Synchronization ...... Unsynchronized
    Last Run ........... -
      1 .................. Unconfigured
      2 .................. Unconfigured
Current Action ......... Idle
  Started ............. -
  Current Node ........ -

---------------------------------------------------------------
<table>
<thead>
<tr>
<th>Node Name</th>
<th>Date</th>
<th>Time</th>
<th>In ATMF</th>
<th>On Media</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>device3</td>
<td>-</td>
<td>-</td>
<td>No</td>
<td>Yes</td>
<td>Prov</td>
</tr>
<tr>
<td>device1</td>
<td>01 Jan 2014 00:05:49</td>
<td>No</td>
<td>Yes</td>
<td>Good</td>
<td></td>
</tr>
<tr>
<td>device2</td>
<td>01 Jan 2014 00:05:44</td>
<td>Yes</td>
<td>Yes</td>
<td>Good</td>
<td></td>
</tr>
</tbody>
</table>
---------------------------------------------------------------
```
atmf provision node configure boot config

**Overview**
This command sets the configuration file to use during the next boot cycle. This command can also set a backup configuration file to use if the main configuration file cannot be accessed for an AMF provisioned node. To unset the boot configuration or the backup boot configuration use the `no boot` command.

Use the **no** variant of this command to set back to the default.

**Syntax**
```
atmf provision node <nodename> configure boot config [backup] [<file-path|URL>]
atmf provision node [<nodename>] configure no boot config [backup]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;nodename&gt;</code></td>
<td>The name of the provisioned node.</td>
</tr>
<tr>
<td>`&lt;file-path</td>
<td>URL&gt;`</td>
</tr>
</tbody>
</table>

**Default**
No boot configuration files or backup configuration files are specified for the provisioned node.

**Mode**
Privileged Exec

**Usage**
When using this command to set a backup configuration file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

**Examples**
To set the configuration file `branch.cfg` on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot config branch.cfg
```

To set the configuration file `backup.cfg` as the backup to the main configuration file on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot config backup usb:/atmf/amf_net/nodes/node1/config/backup.cfg
```

To unset the boot configuration, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot config
```

To unset the backup boot configuration, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot config backup
```
Related Commands

atmf provision node configure boot system
show atmf provision nodes
Overview
This command sets the release file that will load onto a specified provisioned node during the next boot cycle. This command can also set the backup release file to be loaded for an AMF provisioned node. To unset the boot system release file or the backup boot release file use the no boot command.

Use the no variant of this command to set back to the default.

This command can only be run on AMF master nodes.

Syntax
```
atmf provision node <nodename> configure boot system [backup] [<file-path|URL>]
atmf provision node <nodename> configure no boot system [backup]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;nodename&gt;</td>
<td>The name of the provisioned node.</td>
</tr>
<tr>
<td>&lt;file-path</td>
<td>URL&gt;</td>
</tr>
</tbody>
</table>

Default
No boot release file or backup release files are specified for the provisioned node.

Mode
Privileged Exec

Usage
When using this command to set a backup release file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

Examples
To set the release file x610-5.4.4-1.rel on the AMF provisioned node node1, use the command:

```
MasterNodeName# atmf provision node node1 configure boot system x610-5.4.4-1.rel
```

To set the backup release file x610-5.4.4-1.rel as the backup to the main release file on the AMF provisioned node node1, use the command:

```
MasterNodeName# atmf provision node node1 configure boot system backup card:/atmf/amf_net/nodes/node1/flash/x610-5.4.4-1.rel
```

To unset the boot release, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot system
```

To unset the backup boot release, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot system backup
```
Related Commands

- `atmf provision node configure boot config`
- `show atmf provision nodes`
**Overview**

This command sets up an empty directory on the backup media for use with a provisioned node. This directory can have configuration and release files copied to it from existing devices. Alternatively, the configuration files can be created by the user.

An alternative way to create a new provisioned node is with the command `atmf provision node clone`.

This command can only run on AMF master nodes.

**Syntax**

```
atmf provision node <nodename> create
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;nodename&gt;</td>
<td>The name of the node that is being provisioned.</td>
</tr>
</tbody>
</table>

**Mode**

Privileged Exec

**Usage**

This command is only available on master nodes in the AMF network.

The `atmf provision node create` command (or `atmf provision node clone`) must be executed before you can use other `atmf provision node` commands with the specified node name. If a backup or provisioned node already exists for the specified node name then you must delete it before using this command.

A date and time is assigned to the new provisioning directory reflecting when this command was executed. If there is a backup or provisioned node with the same name on another AMF master then the most recent one will be used.

**Example**

To create a new provisioned node named `device2` use the command:

```
device1# atmf provision node device2 create
```

Running this command will create the following directories:

- `<media>:atmf/<atmf_name>/nodes/<node>`
- `<media>:atmf/<atmf_name>/nodes/<node>/flash`

To confirm the new node’s settings, use the command:

```
device1# show atmf backup
```

The output for the `show atmf backup` command is shown in the following figure, and shows details for the new provisioned node `device2`. 
Figure 45-3: Sample output from the `show atmf backup` command

```plaintext
device1# show atmf backup

Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
Next Backup Time .... 02 Jan 2014 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7315.2MB)
Server Config .........
  Synchronization ..... Unsynchronized
    Last Run .......... -
    1 .................. Unconfigured
    2 .................. Unconfigured
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

---------------------------------------------------------------
<table>
<thead>
<tr>
<th>Node Name</th>
<th>Date</th>
<th>Time</th>
<th>In ATMF</th>
<th>On Media</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>device2</td>
<td>-</td>
<td>-</td>
<td>No</td>
<td>Yes</td>
<td>Prov</td>
</tr>
<tr>
<td>device1</td>
<td>01 Jan 2014</td>
<td>00:05:49</td>
<td>No</td>
<td>Yes</td>
<td>Good</td>
</tr>
</tbody>
</table>

For instructions on how to configure on a provisioned node, see the AMF Feature Overview and Configuration Guide.

Related commands
```

atmf provision node clone
ATMF PROVISION NODE DELETE

Overview
This command deletes files that have been created for loading onto a provisioned node. It can only be run on master nodes.

Syntax
atmf provision node <nodename> delete

Mode
Privileged Exec

Usage
This command is only available on master nodes in the AMF network. The command will only work if the provisioned node specified in the command has already been set up (although the device itself is still yet to be installed). Otherwise, an error message is shown when the command is run.

You may want to use the `atmf provision node delete` command to delete a provisioned node that was created in error or that is no longer needed.

This command cannot be used to delete backups created by the AMF backup procedure. In this case, use the command `atmf backup delete` to delete the files.

**NOTE:** This command allows provisioned entries to be deleted even if they have been referenced by the `atmf provision` command, so take care to only delete unwanted entries.

Example
To delete backup files for a provisioned node named device3 use the command:

device1# atmf provision node device3 delete

To confirm that the backup files for provisioned node device3 have been deleted use the command:

device1# show atmf backup

The output should show that the provisioned node device3 no longer exists in the backup file, as shown in the figure below:
Figure 45-4: Sample output showing the `show atmf backup` command

```
device1# show atmf backup

Scheduled Backup ...... Enabled
  Schedule .............. 1 per day starting at 03:00
Next Backup Time ...... 01 Jan 2014 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7297.0MB)
Server Config ..........
  Synchronization ...... Unsynchronized
  Last Run .............. -
  1 ........................ Unconfigured
  2 ........................ Unconfigured
Current Action .......... Idle
  Started ................ -
  Current Node ........... -

---------------------------------------------------------------

<table>
<thead>
<tr>
<th>Node Name</th>
<th>Date</th>
<th>Time</th>
<th>In ATMF</th>
<th>On Media</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>device1</td>
<td>01 Jan 2014</td>
<td>00:05:49</td>
<td>No</td>
<td>Yes</td>
<td>Good</td>
</tr>
<tr>
<td>device2</td>
<td>01 Jan 2014</td>
<td>00:05:44</td>
<td>Yes</td>
<td>Yes</td>
<td>Good</td>
</tr>
</tbody>
</table>

```

Related commands

`atmf provision node create`
**Overview**

This command is used to set up the license certificate for a provisioned node. The certificate file usually has all the license details for the network, and can be stored anywhere in the network. This command makes a hidden copy of the certificate file and stores it in the space set up for the provisioned node on AMF backup media.

For node provisioning, the new device has not yet been part of the AMF network, so the user is unlikely to know its product ID or its MAC address. When such a device joins the network, assuming that this command has been applied successfully, the copy of the certificate file will be applied automatically to the provisioned node.

Once the new device has been resurrected on the network and the certificate file has been downloaded to the provisioned node, the hidden copy of the certificate file is deleted from AMF backup media.

Use the **no** variant of this command to set it back to the default.

This command can only be run on AMF master nodes.

**Syntax**

```
Atmf provision node {<nodename>} license-cert <file-path|URL>
```

```
no atmf provision node {<nodename>} license-cert
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;nodename&gt;</code></td>
<td>The name of the provisioned node.</td>
</tr>
<tr>
<td>`&lt;file-path</td>
<td>URL&gt;`</td>
</tr>
</tbody>
</table>

**Default**

No license certificate file is specified for the provisioned node.

**Mode**

Privileged Exec

**Usage**

This command is only available on master nodes in the AMF network. It will only operate if the provisioned node specified in the command has already been set up, and if the license certification is present in the backup file. Otherwise, an error message is shown when the command is run.

**Example 1**

To apply the license certificate cert1.txt stored on tftp server for AMF provisioned node `device2`, use the command:

```
device1# atmf provision node device2 license-cert
tftp://192.168.1.1/cert1.txt
```
Example 2  To apply the license certificate cert2.txt stored on AMF master's flash directory for AMF provisioned node host2, use the command:

```
device1# atmf provision node device2 license-cert/cert2.txt
```

To confirm that the license certificate has been applied to the provisioned node, use the command `show atmf provision nodes`. The output from this command is shown below, and displays license certification details in the last line.

Figure 45-5: Sample output from the `show atmf provision nodes` command

```plaintext
device1#show atmf provision nodes

ATMF Provisioned Node Information:

Backup Media .............: SD (Total 3827.0MB, Free 3481.1MB)
Node Name : device2
Date & Time : 06-May-2014 & 23:25:44
Provision Path : card:/atmf/nodes

Boot configuration :
Current boot image : x510-1766_atmf_backup.rel (file exists)
Backup boot image : x510-main-20140113-2.rel (file exists)
Default boot config : flash:/default.cfg (file exists)
Current boot config : flash:/abc.cfg (file exists)
Backup boot config : flash:/xyz.cfg (file exists)

Software Licenses :
Repository file : ./configs/.sw_v2.lic
                 : ./configs/.swfeature.lic
Certificate file : card:/atmf/lok/nodes/awplus1/flash/.atmf-lic-cert
```

Related commands `show atmf provision nodes`
atmf provision node locate

**Overview**  
This command changes the present working directory to the directory of a provisioned node. This makes it easier to edit files and create a unique provisioned node in the backup.

This command can only be run on AMF master nodes.

**Syntax**  
`atmf provision node <nodename> locate`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;nodename&gt;</code></td>
<td>The name of the provisioned node.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec

**Usage**  
This command is only available on master nodes in the AMF network. The command will only work if the provisioned node specified in the command has already been set up. Otherwise, an error message is shown when the command is run.

*NOTE: We advise that after running this command, you return to a known working directory, typically flash.*

**Example**  
To change the working directory that happens to be on device1 to the directory of provisioned node device2, use the following command:

```
device1# atmf provision node device2 locate
```

The directory of the node device2 should now be the working directory. You can use the command `pwd` to check this, as shown in the following figure.

**Figure 45-6: Sample output from the `pwd` command**

```
device2#pwd
card:/atmf/building_2/nodes/device2/flash
```

The output above shows that the working directory is now the flash of device2.

**Related commands**  
- `atmf provision node create`
- `atmf provision node node clone`
- `pwd`
atmf reboot-rolling

**Overview**  This command enables you to reboot the nodes in an AMF working-set, one at a time, as a rolling sequence in order to minimize downtime. Once a rebooted node has finished running its configuration and its ports are up, it re-joins the AMF network and the next node is rebooted.

By adding the `url` parameter, you can also upgrade your devices' software one AMF node at a time.

The `force` command enforces a node reboot even if a previous node does not rejoin the AMF network. In this situation the unsuitable node will time-out and the rolling reboot process stops. However, with the `force` parameter applied, the process will ignore the timeout and move on to reboot the next node in the sequence.

This command can take a significant amount of time to complete.

**Syntax**

```
atmf reboot-rolling [force] [<url>]
```

**Parameter**  **Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>force</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;url&gt;</td>
<td>The path to the software upgrade file.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Usage**

You can load the software from a variety of locations. The latest compatible release for a node will be selected from your selected location - based on the parameters and URL you have entered.

For example `card:/5.4.3/x*-5.4.3-*rel` will select from the folder `card:/5.4.3` the latest file that matches the selection `x` (wildcard) `-5.4.3-(wildcard).rel`. Because `x*` is applied, each device type will be detected and its appropriate release file will be installed.

Other allowable entries are:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Used when loading software</th>
</tr>
</thead>
<tbody>
<tr>
<td>card:*rel:</td>
<td>from an SD card</td>
</tr>
<tr>
<td>tftp:&lt;ip-address&gt;:</td>
<td>from a TFTP server</td>
</tr>
<tr>
<td>usb:</td>
<td>from a USB flash drive</td>
</tr>
<tr>
<td>flash:</td>
<td>from flash memory, e.g. from one x610 switch to another</td>
</tr>
<tr>
<td>scp:</td>
<td>using secure copy</td>
</tr>
<tr>
<td>http:</td>
<td>from an HTTP file server</td>
</tr>
</tbody>
</table>
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.
**Example 2**  To update firmware releases, use the following command:

```
Node_1# atmf working-set group all
ATMF_NETWORK[9]# atmf reboot-rolling
card:/5.4.3/x*-5.4.3-*.rel
```
### AMF Commands

#### ATMF REBOOT-ROLLING

ATMF Rolling Reboot Nodes:

<table>
<thead>
<tr>
<th>Node Name</th>
<th>Timeout (Minutes)</th>
<th>New Release File</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW_Team1</td>
<td>8</td>
<td>x510-5.4.3-0.5.rel</td>
<td>Release Ready</td>
</tr>
<tr>
<td>SW_Team2</td>
<td>10</td>
<td>x510-5.4.3-0.5.rel</td>
<td>Release Ready</td>
</tr>
<tr>
<td>SW_Team3</td>
<td>8</td>
<td>---</td>
<td>Not Supported</td>
</tr>
<tr>
<td>HW_Team1</td>
<td>6</td>
<td>---</td>
<td>Incompatible</td>
</tr>
<tr>
<td>Bld1_Floor_2</td>
<td>2</td>
<td>x610-5.4.3-0.5.rel</td>
<td>Release Ready</td>
</tr>
<tr>
<td>Bld1_Floor_1</td>
<td>4</td>
<td>---</td>
<td>Incompatible</td>
</tr>
<tr>
<td>Building_1</td>
<td>2</td>
<td>---</td>
<td>Incompatible</td>
</tr>
<tr>
<td>Building_2</td>
<td>2</td>
<td>x908-5.4.3-0.5.rel</td>
<td>Release Ready</td>
</tr>
</tbody>
</table>

Continue upgrading releases? (y/n):
AMF COMMANDS

ATMF RECOVER

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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;node-name&gt;</td>
<td>The name of the device whose configuration is to be recovered or replicated.</td>
</tr>
<tr>
<td>master &lt;node-name&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>controller &lt;node-name&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

Mode
Privileged Exec

Usage
The recovery/replication process involves loading the configuration file for a node that is either about to be replaced or has experienced some problem. You can specify the configuration file of the device being replaced by using the <node-name> parameter, and you can specify the name of the master node or controller holding the configuration file.

If the <node-name> parameter is not entered then the node will attempt to use one that has been previously configured. If the replacement node has no previous configuration (and has no previously used node-name), then the recovery will fail.

If the master or controller name is not specified then the device will poll all known AMF masters and controllers and execute an election process (based on the last successful backup and its timestamp) to determine which to use. If no valid backup master or controller is found, then this command will fail.

No error checking occurs when this command is run. Regardless of the last backup status, the recovering node will attempt to load its configuration from the specified master node or controller.

If the node has previously been configured, we recommend that you suspend any AMF backup before running this command. This is to prevent corruption of the backup files on the AMF master as it attempts to both backup and recover the node at the same time.
Example
To recover the AMF node named Node_10 from the AMF master node named Master_2, use the following command:

```
Master_2# atmf recover Node_10 master Master_2
```

Related Commands
- `atmf backup stop`
- `show atmf backup`
- `show atmf`
**Overview**  
This command turns off the recovery failure flashing port LEDs. It reverts the LED's function to their normal operational mode, and in doing so assists with resolving the recovery problem. You can repeat this process until the recovery failure has been resolved. For more information, see the AMF Feature Overview and Configuration Guide.

**Syntax**  
`atmf recover led-off`

**Default**  
Normal operational mode

**Mode**  
Privileged Exec

**Example**  
To revert the LEDs on Node1 from recovery mode display, to their normal operational mode, use the command:

```
Node1# atmf recover led-off
```

**Related Commands**  
`atmf recover`
atmf remote-login

**Overview**  Use this command to remotely login to other AMF nodes in order to run commands as if you were a local user of that node.

**Syntax**  atmf remote-login [user <name>] <nodename>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>User name.</td>
</tr>
<tr>
<td>&lt;nodename&gt;</td>
<td>Node name.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec (This command will only run at privilege level 15)

**Usage**  You do not need a valid login on the local device in order to run this command. The session will take you to the enable prompt on the new device. If the remote login session exits for any reason (i.e. device reboot) you will be returned to the originating node.

The software will not allow you to run multiple remote login sessions. You must exit an existing session before starting a new one.

**Example 1**  To remotely login from node Node10 to Node20 use the following command:

Node10# atmf remote-login node20

**Example 2**  In this example, user Whitney is a valid user of node5. She can remotely login from node5 to node3 by using the following commands:

node5# atmf remote-login user whitney node3
node3> enable

*NOTE:* In the above example the user name whitney is valid on both nodes. Therefore, to prevent unauthorized access, user names should be unique across all nodes within the AMF network.
**atmf restricted-login**

**Overview**  This command restricts the use of the `atmf working-set` on page 1939 command on all AMF master nodes to privilege 15 users only. Once entered on any AMF master node, this command will propagate across the network.

Note that once you have run this command, certain other commands that utilize the AMF working-set command, such as the `include`, `atmf reboot-rolling` and `show atmf group members` commands, will operate only on master nodes.

Use the `no` variant of this command to disable restricted login on the AMF network. This allows access to the `atmf working-set` command from any node in the AMF network.

**Syntax**  

```
atmf restricted-login
no atmf restricted-login
```

**Mode**  Privileged Exec

**Default**  

- Master nodes operate with `atmf restricted-login` disabled.
- Member nodes operate with `atmf restricted-login` enabled.

**NOTE:** The default conditions of this command vary from those applied by its “no” variant. This is because the restricted-login action is only applied by master nodes, and in the absence of a master node, the default is to apply the restricted action to all member nodes with AMF configured.

*In the presence of a master node, its default of “atmf restricted-login disabled” will permeate to all its member nodes. Similarly, any change in this command’s status that is made on a master node, will also permeate to all its member nodes*

**Example**  

To enable restricted login, use the command

```
Node_20(config)# atmf restricted-login node20
```

**Validation Command**  

```
show atmf
```
atmf select-area

Overview
Use this command to access devices in an area outside the core area on the controller network. This command will connect you to the remote area-master of the specified area.

This command is only valid on AMF controllers.

The no variant of this command disconnects you from the remote area-master.

Syntax

```plaintext
atmf select-area {<area-name>|local}

no atmf select-area
```

Mode
Privileged Exec

Usage
After running this command, use the atmf working-set command to select the set of nodes you want to access in the remote area.

Example

To access nodes in the area Canterbury, use the command

```
controller-1# atmf select-area Canterbury
```

This displays the following output:

```
Test_network[3]#atmf select-area Canterbury
----------------------------------------------------------
Connected to area Canterbury via host Avensis:          
----------------------------------------------------------
```

To return to the local area for controller-1, use the command

```
controller-1# atmf select-area local
```

Alternatively, to return to the local area for controller-1, use the command

```
controller-1# no atmf select-area
```

Related
Commands

atmf working-set
**Overview**
This command creates one or more Layer 2 tunnels that enable AMF nodes to transparently communicate across a wide area network using Layer 2 connectivity protocols.

Once connected through the tunnel, the remote member will have the same AMF capabilities as a directly connected AMF member.

Use the `no` variant of this command to remove the specified virtual link.

**Syntax**
```
atmf virtual-link id <1-4094> ip <a.b.c.d> remote-id <1-4094> remote-ip <a.b.c.d> [remote-area <area-name>] no atmf virtual-link id <1-4094>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The Internet Protocol (IP).</td>
</tr>
<tr>
<td>&lt;a.b.c.d&gt;</td>
<td>The IP address, of the local amf node (at its interface to the tunnel) entered in a.b.c.d format.</td>
</tr>
<tr>
<td>remote-id</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;1-4094&gt;</td>
<td>The ID range 1-32.</td>
</tr>
<tr>
<td>remote-ip</td>
<td>The IP address of the remote node</td>
</tr>
<tr>
<td>&lt;a.b.c.d&gt;</td>
<td>The IP address, of the remote node (at its interface to the tunnel) entered in a.b.c.d format.</td>
</tr>
<tr>
<td>remote-area</td>
<td>The remote area connected to this area virtual link</td>
</tr>
<tr>
<td>&lt;area-name&gt;</td>
<td>The name of the remote area connected to this virtual link.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Usage**
The Layer 2 tunnel that this command creates enables a local AMF session to appear to pass transparently across a Wide Area Network (WAN) such as the Internet. The addresses configured as the local and remote tunnel IP addresses must have IP connectivity to each other. If the tunnel is configured to connect a head office and branch office over the Internet, typically this would involve using some type of managed WAN service such as a site-to-site VPN. Tunnels are only supported using IPv4.

Configuration involves creating a local tunnel ID, a local IP address, a remote tunnel ID and a remote IP address. A reciprocal configuration is also required on the corresponding remote device. The local tunnel ID must be unique to the device on which it is configured.
The tunneled link may operate via external (non AlliedWare Plus) routers in order to provide wide area network connectivity. However in this configuration, the routers perform a conventional router to router connection. The protocol tunneling function is accomplished by the AMF nodes.

**NOTE:** The requirement to pre-configure the local IP address and tunnel ID on a device located at the far end of an AMF virtual-link tunnel means that zero touch device replacement cannot be achieved on a remote device that terminates the tunnel connection.

**Example 1** Use the following commands to create the tunnel shown in the figure below.

Figure 45-7: AMF virtual link example

```
Node_10(config)# atmf virtual-link id 1 ip 192.168.1.1
remote-id 2 remote-ip 192.168.2.1

Node_20(config)# atmf virtual-link id 2 ip 192.168.2.1
remote-id 1 remote-ip 192.168.1.1
```

**Example 2** To set up an area virtual link to a remote site (assuming IP connectivity between the sites already), one site must run the following commands:

```
SiteA# configure terminal
SiteA(config)# atmf virtual-link id 5 ip 192.168.100.1
remote-id 10 remote-ip 192.168.200.1 remote-area SiteB-AREA
```

The second site must run the following commands:

```
SiteB# configure terminal
SiteB(config)# atmf virtual-link id 10 ip 192.168.200.1
remote-id 5 remote-ip 192.168.100.1 remote-area SiteA-AREA
```

**Validation Command** `show atmf`

Before you can apply the above `atmf virtual-link` command, you must configure the area names `SiteB-AREA` and `SiteA-AREA`. 
show atmf links
atmf working-set

**Overview**  The AMF working-set command enables you to execute commands across an individually listed set (or preselected group) of AMF nodes. Group selection is made using the `atmf group` (membership) command.

This command opens a session on multiple network devices. When you change the working set to anything other than the local device, the prompt will change to the AMF network name, followed by the size of the working set, shown in square brackets. This command has to be run at privilege level 15.

In addition to the user defined groups, the following system assigned groups are automatically created:

- Implicit Groups
  - local: The originating node.
  - current: All nodes that comprise the current working-set
  - all: All nodes in the AMF

- Automatic Groups - These can be defined by hardware architecture, e.g. x510, x610, x8100, AR3050S or AR4050S, or by certain AMF nodal designations such as master.

Note that the Implicit Groups do not appear in show group output.

If a node is an AMF master it will be automatically added to the master group.

**Syntax**

```
atmf working-set
{[<node-list>]}[group{<group-list>|all|local|current}]}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;node-list&gt;</code></td>
<td>A comma delimited list (without spaces) of nodes to be included in the working-set.</td>
</tr>
<tr>
<td>group</td>
<td>The AMF group.</td>
</tr>
<tr>
<td><code>&lt;group-list&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td>all</td>
<td>All nodes in the AMF.</td>
</tr>
<tr>
<td>local</td>
<td>Local node Running this command with the parameters <strong>group local</strong> will return you to the local prompt and local node connectivity.</td>
</tr>
<tr>
<td>current</td>
<td>Nodes in current list.</td>
</tr>
</tbody>
</table>

**Default**  Needs to be entered

**Mode**  Privileged Exec
**Example 1**

To add all nodes in the AMF to the working-set, use the command:

```
node1# atmf working-set group all
```

**NOTE:** *This command adds the implicit group “all” to the working set, where “all” comprises all nodes in the AMF.*

This command displays an output screen similar to the one shown below:

```
node1, node2, node3, node4, node5, node6: ________________________________________________________________
Working set join
ATMF_NETWORK_Name[6]#
```

**Example 2**

To return to the local prompt, and connectivity to only the local node; use the command:

```
ATMF_NETWORK_Name[6]# atmf working-set group local
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1, node2</td>
<td>The name of the nodes - as set by the hostname command.</td>
</tr>
<tr>
<td>ATMF_Network_Name</td>
<td>The name of the AMF network - as set by the atmf network-name command.</td>
</tr>
</tbody>
</table>
clear atmf links statistics

Overview
This command resets the values of all AMF link, port, and global statistics to zero.

Syntax
clear atmf links statistics

Mode
Privilege Exec

Example
To reset the AMF link statistics values, use the command:

```
node_1# clear atmf links statistics
```

Related Commands
show atmf links statistics
**debug atmf**

**Overview**  
This command enables the AMF debugging facilities, and displays information that is relevant (only) to the current node. The detail of the debugging displayed depends on the parameters specified.

If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

The **no** variant of this command disables either all AMF debugging information, or only the particular information as selected by the command’s parameters.

**Syntax**
```
debug atmf
[link|crosslink|arealink|database|neighbor|error|all]
```
```
no debug atmf
[link|crosslink|arealink|database|neighbor|error|all]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>link</td>
<td>Output displays debugging information relating to uplink or downlink information.</td>
</tr>
<tr>
<td>crosslink</td>
<td>Output displays all crosslink events.</td>
</tr>
<tr>
<td>arealink</td>
<td>Output displays all arealink events.</td>
</tr>
<tr>
<td>database</td>
<td>Output displays only notable database events.</td>
</tr>
<tr>
<td>neighbor</td>
<td>Output displays only notable AMF neighbor events.</td>
</tr>
<tr>
<td>error</td>
<td>Output displays AMF error events.</td>
</tr>
<tr>
<td>all</td>
<td>Output displays all AMF events.</td>
</tr>
</tbody>
</table>

**Default**  
All debugging facilities are disabled.

**Mode**  
User Exec and Global Configuration

**Usage**  
If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

**NOTE:** An alias to the **no** variant of this command is **undebug atmf** on page 2004.

**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**  
```
d 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>]
```

```
d 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 Rx and Tx, 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**  If no additional parameters are specified, then the command output will apply a default selection of parameters shown below:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>direction</td>
<td>Sets debug to packet received, transmitted, or both</td>
</tr>
<tr>
<td>rx</td>
<td>packets received by this node</td>
</tr>
<tr>
<td>tx</td>
<td>Packets sent from this node</td>
</tr>
<tr>
<td>1</td>
<td>AMF Packet Control header Information, Packet Sequence Number. Enter 1 to select this level.</td>
</tr>
<tr>
<td>2</td>
<td>AMF Detailed Packet Information. Enter 2 to select this level.</td>
</tr>
<tr>
<td>3</td>
<td>AMF Packet HEX dump. Enter 3 to select this level.</td>
</tr>
</tbody>
</table>
AMF COMMANDS
DEBUG ATMF PACKET

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout</td>
<td>Sets the execution timeout for packet logging</td>
</tr>
<tr>
<td>&lt;seconds&gt;</td>
<td>Seconds</td>
</tr>
<tr>
<td>num-pkts</td>
<td>Sets the number of packets to be dumped</td>
</tr>
<tr>
<td>&lt;quantity&gt;</td>
<td>The actual number of packets</td>
</tr>
<tr>
<td>filter</td>
<td>Sets debug to filter packets</td>
</tr>
<tr>
<td>node</td>
<td>Sets the filter on packets for a particular Node</td>
</tr>
<tr>
<td>&lt;name&gt;</td>
<td>The name of the remote node</td>
</tr>
<tr>
<td>interface</td>
<td>Sets the filter to dump packets from an interface (portx.x.x) on the local node</td>
</tr>
<tr>
<td>&lt;ifname&gt;</td>
<td>Interface port or virtual-link</td>
</tr>
<tr>
<td>pkt-type</td>
<td>Sets the filter on packets with a particular AMF packet type</td>
</tr>
<tr>
<td>1</td>
<td>Crosslink Hello BPDU packet with crosslink links information. Enter 1 to select this packet type.</td>
</tr>
<tr>
<td>2</td>
<td>Crosslink Hello BPDU packet with downlink domain information. Enter 2 to select this packet type.</td>
</tr>
<tr>
<td>3</td>
<td>Crosslink Hello BPDU packet with uplink information. Enter 3 to select this packet type.</td>
</tr>
<tr>
<td>4</td>
<td>Downlink and uplink hello BPDU packets. Enter 4 to select this packet type.</td>
</tr>
<tr>
<td>5</td>
<td>Non broadcast hello unicast packets. Enter 5 to select this packet type.</td>
</tr>
<tr>
<td>6</td>
<td>Stack hello unicast packets. Enter 6 to select this packet type.</td>
</tr>
<tr>
<td>7</td>
<td>Database description. Enter 7 to select this packet type.</td>
</tr>
<tr>
<td>8</td>
<td>DBE request. Enter 8 to select this packet type.</td>
</tr>
<tr>
<td>9</td>
<td>DBE update. Enter 9 to select this packet type.</td>
</tr>
<tr>
<td>10</td>
<td>DBE bitmap update. Enter 10 to select this packet type.</td>
</tr>
<tr>
<td>11</td>
<td>DBE acknowledgment. Enter 11 to select this packet type.</td>
</tr>
<tr>
<td>12</td>
<td>Area Hello Packets. Enter 12 to select this packet type.</td>
</tr>
<tr>
<td>13</td>
<td>Gateway Hello Packets. Enter 13 to select this packet type.</td>
</tr>
</tbody>
</table>

**Examples**

To set a packet debug on node 1 with level 1 and no timeout, use the command:

```
node_1# debug atmf packet direction tx timeout 0
```

To set a packet debug with level 3 and filter packets received from AMF node 1:

```
node_1# debug atmf packet direction tx level 3 filter node_1
```
To enable send and receive 500 packets only on vlink1 for packet types 1, 7, and 11, use the command:

```
node_1# debug atmf packet num-pkts 500 filter interface vlink1 pkt-type 1 7 11
```

This example applies the `debug atmf packet` command and combines many of its options:

```
node_1# debug atmf packet direction rx level 1 num-pkts 60 filter node x610 interface port1.0.1 pkt-type 4 7 10
```
erase factory-default

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

- The current release file and its /flash/.release file
- The backup release file and /flash/backup file
- v1 license files /flash/.configs/.swfeature.lic
- v2 license files /flash/.configs/.sw_v2.lic

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

**Syntax**  `erase factory-default`

**Mode**  Global Configuration.

**Usage**  This command is an alias to the `atmf cleanup` command.

**Example**  To erase data, use the command:

Node_1(config)# erase factory-default

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

**Related Commands**  `atmf cleanup`
show atmf

**Overview**  Displays information about the current AMF node.

**Syntax**  

```
show atmf [summary|tech|nodes|session]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Displays summary information about the current AMF node.</td>
</tr>
<tr>
<td>tech</td>
<td>Displays global AMF information.</td>
</tr>
<tr>
<td>nodes</td>
<td>Displays a list of AMF nodes together with brief details.</td>
</tr>
<tr>
<td>session</td>
<td>Displays information on an AMF session.</td>
</tr>
</tbody>
</table>

**Default**  Only summary information is displayed.

**Mode**  User Exec and Privileged Exec

**Usage**  AMF uses internal VLANs to communicate between nodes about the state of the AMF network. Two VLANs have been selected specifically for this purpose. Once these have been assigned, they are reserved for AMF and cannot be used for other purposes.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Example 1**  To show summary information on AMF node_1 use the following command:

```
node_1# show atmf summary
```

The following figure shows some example output from running this command for a specific AMF node.

Table 45-1: Output from the **show atmf summary** command

```
node_1#show atmf summary
ATMF Summary Information:
ATMF Status             : Enabled
Network Name            : Test_network
Node Name               : node_1
Role                    : Controller
Role                    : Master
Restricted login        : Disabled
Current ATMF Nodes      : 3
```

**Example 2**  To show information specific to AMF nodes use the following command:

```
node_1# show atmf nodes
```
The **show amf session** command displays all CLI (Command Line Interface) sessions for users that are currently logged in and running a CLI session. For example, in the case below, node_1 and node5 have active users logged in.

**Example 3**  
To display AMF active sessions, use the following command:

```
node_1# show atmf session
```

**Table 45-2: Output from the `show atmf session` command**

| Session ID | : 73518  |
| Node Name  | : node_1 |
| PID        | : 7982   |
| Link type  | : Broadcast-cli |
| MAC Address| : 0000.0000.0000 |
| Options    | : 0      |
| Our bits   | : 0      |
| Link State | : Full   |
| Domain Controller | : 0 |
| Backup Domain Controller | : 0 |
| Database Description Sequence Number | : 00000000 |
| First Adjacency | : 1 |
| Number Events | : 0 |
| DBE Retransmit Queue Length | : 0 |
| DBE Request List Length | : 0 |

| Session ID | : 410804  |
| Node Name  | : node5  |
| PID        | : 17588  |
| Link type  | : Broadcast-cli |
| MAC Address| : 001a.eb56.9020 |
| Options    | : 0      |
| Our bits   | : 0      |
| Link State | : Full   |
| Domain Controller | : 0 |
| Backup Domain Controller | : 0 |
| Database Description Sequence Number | : 00000000 |
| First Adjacency | : 1 |
| Number Events | : 0 |
| DBE Retransmit Queue Length | : 0 |
| DBE Request List Length | : 0 |

The AMF tech command collects all the AMF commands, and displays them. You can use this command when you want to see an overview of the AMF network.

**Example 4**  
To display AMF technical information, use the following command:

```
node_1# show atmf tech
```
Table 45-3: Output from the **show atmf tech** command

```
node_1#show atmf tech
ATMF Summary Information:
ATMF Status : Enabled
Network Name : ATMF_NET
Node Name : node_1
Role : Master
Current ATMF Nodes : 8

ATMF Technical information:
Network Name : ATMF_NET
Domain : node_1's domain
Node Depth : 0
Domain Flags : 0
Authentication Type : 0
MAC Address : 0014.2299.137d
Board ID : 287
Domain State : DomainController
Domain Controller : node_1
Backup Domain Controller : node2
Domain controller MAC : 0014.2299.137d
Parent Domain : -
Parent Domain Controller : -
Parent Domain Controller MAC : 0000.0000.0000
Number of Domain Events : 0
Crosslink Ports Blocking : 0
Uplink Ports Waiting on Sync : 0
Crosslink Sequence Number : 7
Domains Sequence Number : 28
Uplink Sequence Number : 2
Number of Crosslink Ports : 1
Number of Domain Nodes : 2
Number of Neighbors : 5
Number of Non Broadcast Neighbors : 3
Number of Link State Entries : 1
Number of Up Uplinks : 0
Number of Up Uplinks on This Node : 0
DBE Checksum : 84fc6
Number of DBE Entries : 0
Management Domain Ifindex : 4391
Management Domain VLAN : 4091
Management ifindex : 4392
Management VLAN : 4092
```

Table 45-4: Parameter definitions from the **show atmf tech** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATMF Status</td>
<td>The Node's AMF status, either Enabled or Disabled.</td>
</tr>
<tr>
<td>Network Name</td>
<td>The AMF network that a particular node belongs to.</td>
</tr>
<tr>
<td>Node Name</td>
<td>The name assigned to a particular node.</td>
</tr>
</tbody>
</table>
### AMF Commands

#### SHOW ATMF

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>The role configured for this AMF device, either Master or Member.</td>
</tr>
<tr>
<td>Current ATMF Nodes</td>
<td>The count of AMF nodes in an AMF Network.</td>
</tr>
<tr>
<td>Node Address</td>
<td>An Address used to access a remotely located node (.atmf).</td>
</tr>
<tr>
<td>Node ID</td>
<td>A Unique identifier assigned to a Node on an AMF network.</td>
</tr>
<tr>
<td>Node Depth</td>
<td>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.</td>
</tr>
<tr>
<td>Domain State</td>
<td>The state of Node in a Domain in AMF network as Controller/Backup.</td>
</tr>
<tr>
<td>Recovery State</td>
<td>The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.</td>
</tr>
<tr>
<td>Management VLAN</td>
<td>The VLAN created for traffic between Nodes of different domain (up/down links). &lt;ul&gt; &lt;li&gt;VLAN ID - In this example VLAN 4092 is configured as the Management VLAN.&lt;/li&gt; &lt;li&gt;Management Subnet - Network prefix for the subnet.&lt;/li&gt; &lt;li&gt;Management IP Address - The IP address allocated for this traffic.&lt;/li&gt; &lt;li&gt;Management Mask - The subnet mask used to create a subnet for this traffic (255.255.128.0). &lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>Domain VLAN</td>
<td>The VLAN assigned for traffic between Nodes of same domain (crosslink). &lt;ul&gt; &lt;li&gt;VLAN ID - In this example VLAN 4091 is configured as the domain VLAN.&lt;/li&gt; &lt;li&gt;Domain Subnet. The subnet address used for this traffic.&lt;/li&gt; &lt;li&gt;Domain IP Address. The IP address allocated for this traffic.&lt;/li&gt; &lt;li&gt;Domain Mask. The subnet mask used to create a subnet for this traffic (255.255.128.0). &lt;/li&gt;&lt;/ul&gt;</td>
</tr>
<tr>
<td>Device Type</td>
<td>The Product Series name.</td>
</tr>
<tr>
<td>ATMF Master</td>
<td>Whether the node is an AMF master node for its area ('Y' if it is and 'N' if it is not).</td>
</tr>
<tr>
<td>SC</td>
<td>The device configuration, one of C - Chassis (SBx8100 Series), S - Stackable (VCS) or N - Standalone.</td>
</tr>
<tr>
<td>Parent</td>
<td>The node to which the current node has an active uplink.</td>
</tr>
<tr>
<td>Node Depth</td>
<td>The number of nodes in the path from this node to the master node.</td>
</tr>
</tbody>
</table>

**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>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>detail</code></td>
<td>Displays detailed information</td>
</tr>
<tr>
<td><code>&lt;area-name&gt;</code></td>
<td>Displays information about master and gateway nodes in the specified area only.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec

**Example 1**  
To show information about all areas, use the command:

```bash
controller-1# show atmf area
```

The following figure shows example output from running this command on a controller.

Table 45-5: Example output from the `show atmf area` command on a Controller.

<table>
<thead>
<tr>
<th>Area Name</th>
<th>Area</th>
<th>Local</th>
<th>Remote Gateway</th>
<th>Remote Master</th>
<th>Node Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wellington</td>
<td>2</td>
<td>Reachable</td>
<td>Reachable</td>
<td>Auth OK</td>
<td>120</td>
</tr>
<tr>
<td>Canterbury</td>
<td>3</td>
<td>Reachable</td>
<td>Reachable</td>
<td>Auth Error</td>
<td>-</td>
</tr>
<tr>
<td>SiteA-AREA</td>
<td>14</td>
<td>Unreachable</td>
<td>Unreachable</td>
<td>Unreachable</td>
<td>-</td>
</tr>
<tr>
<td>Auckland</td>
<td>100</td>
<td>Reachable</td>
<td>Reachable</td>
<td>Auth Start</td>
<td>-</td>
</tr>
<tr>
<td>Southland</td>
<td>120</td>
<td>Reachable</td>
<td>Reachable</td>
<td>Auth OK</td>
<td>54</td>
</tr>
</tbody>
</table>

Area count: 6  
Area node count: 177

The following figure shows example output from running this command on a remote master.
Table 45-6: Example output from the **show atmf area** command on a remote master.

<table>
<thead>
<tr>
<th>Area Name</th>
<th>Area ID</th>
<th>Local Gateway</th>
<th>Remote Gateway</th>
<th>Remote Master</th>
<th>Node Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>NZ</td>
<td>1</td>
<td>Reachable</td>
<td>N/A</td>
<td>N/A</td>
<td>-</td>
</tr>
<tr>
<td>* Canterbury</td>
<td>3</td>
<td>Reachable</td>
<td>N/A</td>
<td>N/A</td>
<td>40</td>
</tr>
</tbody>
</table>

**ATMF Area Information:**

* = Local area

---

**Area Count:** 2

**Local area node count:** 40

Table 45-7: Parameter definitions from the **show atmf area** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Indicates the area of the device on which the command is being run.</td>
</tr>
<tr>
<td>Area Name</td>
<td>The name of each area.</td>
</tr>
<tr>
<td>Area ID</td>
<td>The ID of the area.</td>
</tr>
<tr>
<td>Local Gateway</td>
<td>Whether the local gateway node is reachable or not.</td>
</tr>
<tr>
<td>Remote Gateway</td>
<td>Whether the remote gateway node is reachable or not. This is one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Reachable, if the link has been established.</td>
</tr>
<tr>
<td></td>
<td>• 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 <code>switchport atmf-arealink remote-area</code> command.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Auth Start, which may indicate that the area names match on the controller and remote master, but the IDs do not match.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Auth OK, which indicates that area authentication was successful and you can now use the <code>atmf select-area</code> command.</td>
</tr>
<tr>
<td>Remote Master</td>
<td>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.</td>
</tr>
<tr>
<td>Node Count</td>
<td>The number of nodes in the area.</td>
</tr>
<tr>
<td>Area Count</td>
<td>The number of areas controlled by the controller.</td>
</tr>
<tr>
<td>Area Node Count</td>
<td>The total number of nodes in the area.</td>
</tr>
</tbody>
</table>
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 45-8: Output from the `show atmf area detail` command

```
controller-1# show atmf area detail
ATMF Area Detail Information:
Controller distance : 0
Controller Id : 21
Backup Available : FALSE
Area Id : 2
Gateway Node Name : controller-1
Gateway Node Id : 342
Gateway Ifindex : 6013
Masters Count : 1
Master Node Name : well-master (329)
Node Count : 2

Area Id : 3
Gateway Node Name : controller-1
Gateway Node Id : 342
Gateway Ifindex : 4511
Masters Count : 2
Master Node Name : cant1-master (15)
Master Node Name : cant2-master (454)
Node Count : 2
```

Related Commands
- `show atmf area summary`
- `show atmf area nodes`
- `show atmf area nodes-detail`
show atmf area summary

Overview
Use this command to display a summary of IPv6 addresses used by AMF, for one or all of the areas controlled by an AMF controller.

Syntax
show atmf area summary [<area-name>]

Parameter | Description
--- | ---
area-name | Displays information for the specified area only.

Mode
Privileged Exec

Example 1
To show a summary of IPv6 addresses used by AMF, for all of the areas controlled by controller-1, use the command:

controller-1# show atmf area summary

The following figure shows example output from running this command.

Table 45-9: Output from the `show atmf area summary` command

```
controller-1# show atmf area summary

ATMF Area Summary Information:

Management Information
Local IPv6 Address: fd00:4154:4d46:1::15

Area Information
Area Name: NZ (Local)  Area ID: 1
Area Master IPv6 Address: -

Area Name: Wellington  Area ID: 2
Area Master IPv6 Address: fd00:4154:4d46:2::149

Area Name: Canterbury  Area ID: 3
Area Master IPv6 Address: fd00:4154:4d46:3::f

Area Name: Auckland  Area ID: 100
Area Master IPv6 Address: fd00:4154:4d46:64::17
Interface: vlink2000
```
show atmf area nodes

**Overview**
Use this command to display summarised information about an AMF controller's remote nodes.

**Syntax**
```
show atmf area nodes [ <area-name> ] [ <node-name> ]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-name&gt;</td>
<td>Displays information about nodes in the specified area.</td>
</tr>
<tr>
<td>&lt;node-name&gt;</td>
<td>Displays information about the specified node.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Usage**
If you do not limit the output to a single area or node, this command lists all remote nodes that the controller is aware of. This can be a very large number of nodes.

**Example**
To show summarised information about all the nodes the controller is aware of, use the command:
```
controller-1# show atmf area nodes
```

The following figure shows partial example output from running this command.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Name</td>
<td>The name assigned to a particular node.</td>
</tr>
<tr>
<td>Device Type</td>
<td>The Product series name.</td>
</tr>
</tbody>
</table>
AMF COMMANDS
SHOW ATMF AREA NODES

Table 45-11: Parameter definitions from the **show atmf area nodes** command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATMF Master</td>
<td>Whether the node is an AMF master node for its area ('Y' if it is and 'N' if it is not).</td>
</tr>
<tr>
<td>SC</td>
<td>The device configuration, one of C - Chassis (SBx8100 series), S - Stackable (VCS) or N - Standalone.</td>
</tr>
<tr>
<td>Parent</td>
<td>The node to which the current node has an active uplink.</td>
</tr>
<tr>
<td>Node Depth</td>
<td>The number of nodes in the path from this node to the master node.</td>
</tr>
</tbody>
</table>

**Related Commands**
- show atmf area
- show atmf area nodes-detail
show atmf area nodes-detail

**Overview**
Use this command to display detailed information about an AMF controller's remote nodes.

**Syntax**
```
show atmf area nodes-detail [<area-name>] [<node-name>]
```

**Mode**
Privileged Exec

**Usage**
If you do not limit the output to a single area or node, this command displays information about all remote nodes that the controller is aware of. This can be a very large number of nodes.

**Example**
To show information about all the nodes the controller is aware of, use the command:

```
controller-1# show atmf area nodes-detail
```

The following figure shows partial example output from running this command.

Table 45-12: Output from the show atmf area nodes-detail command

```
controller-1# show atmf area nodes-detail
Wellington Area Node Information:
  Node name  well-gate
  Parent node name  well-master
  Domain id  well-gate’s domain
  Board type  368
  Distance to core  1
  Flags  50
  Extra flags  0x00000006
  MAC Address  001a.eb56.9020

Node name well-master
  Parent node name  none
  Domain id  well-master’s domain
  Board type  333
  Distance to core  0
  Flags  51
  Extra flags  0x0000000c
  MAC Address  eccd.6d3f.fef7
...
```
Table 45-13: Parameter definitions from the `show atmf area nodes-detail` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node name</td>
<td>The name assigned to a particular node.</td>
</tr>
<tr>
<td>Parent node name</td>
<td>The node to which the current node has an active uplink.</td>
</tr>
<tr>
<td>Domain id</td>
<td></td>
</tr>
<tr>
<td>Board type</td>
<td>The Allied Telesis code number for the device.</td>
</tr>
<tr>
<td>Distance to core</td>
<td>The number of nodes in the path from the current node to the master node in its area.</td>
</tr>
<tr>
<td>Flags</td>
<td>Internal AMF information</td>
</tr>
<tr>
<td>Extra flags</td>
<td>Internal AMF information</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the current node</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show atmf area`
- `show atmf area nodes`
show atmf backup

**Overview**  This command displays information about AMF backup status for all the nodes in an AMF network. It can only be run on AMF master and controller nodes.

**Syntax**  
show atmf backup [logs|server-status|synchronize [logs]]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logs</td>
<td>Displays detailed log information.</td>
</tr>
<tr>
<td>server-status</td>
<td>Displays connectivity diagnostics information for each configured remote file server.</td>
</tr>
<tr>
<td>synchronize</td>
<td>Display the file server synchronization status</td>
</tr>
<tr>
<td>logs</td>
<td>For each remote file server, display the logs for the last synchronization</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Example 1**  To display the AMF backup information, use the command:

```
node_1# show atmf backup
```
Example 2  To display the AMF backup information with the optional parameter server-status, use the command:

```
Node_1# show atmf backup server-status
```

<table>
<thead>
<tr>
<th>Id</th>
<th>Last Check</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>186 s</td>
<td>File server ready</td>
</tr>
<tr>
<td>2</td>
<td>1 s</td>
<td>SSH no route to host</td>
</tr>
</tbody>
</table>

Table 45-14: Parameter definitions from the show atmf backup server-status command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Backup</td>
<td>Indicates whether AMF backup scheduling is enabled or disabled.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Displays the configured backup schedule.</td>
</tr>
<tr>
<td>Next Backup Time</td>
<td>Displays the date and time of the next scheduled.</td>
</tr>
</tbody>
</table>
Table 45-14: Parameter definitions from the `show atmf backup server-status` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Media</td>
<td>The current backup medium in use. This will be one of USB, SD, or NONE. Note that the USB will take precedence over the SD card. Utilized and available memory (MB) will be indicated if backup media memory is present.</td>
</tr>
<tr>
<td>Current Action</td>
<td>The task that the AMF backup mechanism is currently performing. This will be a combination of either (Idle, Starting, Doing, Stopping), or (manual, scheduled).</td>
</tr>
<tr>
<td>Started</td>
<td>The date and time that the currently executing task was initiated in the format DD MMM YYYY.</td>
</tr>
<tr>
<td>Current Node</td>
<td>The name of the node that is currently being backed up.</td>
</tr>
<tr>
<td>Node Name</td>
<td>The name of the node that is storing backup data - on its backup media.</td>
</tr>
<tr>
<td>Date</td>
<td>The data of the last backup in the format DD MMM YYYY.</td>
</tr>
<tr>
<td>Time</td>
<td>The time of the last backup in the format HH:MM:SS.</td>
</tr>
<tr>
<td>In ATMF</td>
<td>Whether the node shown is active in the AMF network, (Yes or No).</td>
</tr>
<tr>
<td>Status</td>
<td>The output can contain one of four values:</td>
</tr>
<tr>
<td></td>
<td>• &quot;-&quot; meaning that the status file cannot be found or cannot be read.</td>
</tr>
<tr>
<td></td>
<td>• &quot;Errors&quot; meaning that there are issues - note that the backup may still be deemed successful depending on the errors.</td>
</tr>
<tr>
<td></td>
<td>• &quot;Stopped&quot; meaning that the backup attempt was manually aborted;</td>
</tr>
<tr>
<td></td>
<td>• &quot;Good&quot; meaning that the backup was completed successfully.</td>
</tr>
<tr>
<td>Log File Location</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>card:/amf/office/logs/rsync_amf_testbox1.log.</td>
</tr>
<tr>
<td>Log Details</td>
<td>The contents of the backup log file.</td>
</tr>
<tr>
<td>server-status</td>
<td>Displays connectivity diagnostics information for each configured remove file server.</td>
</tr>
</tbody>
</table>

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Related Commands**
- `show atmf`
- `atmf network-name`
show atmf backup area

Overview
Use this command to display backup status information for the master nodes in one or more areas. This command is only available on AMF controllers.

Syntax
show atmf backup area [logs] [<area-name>] [<node-name>]

Mode
Privileged Exec

Example
To show information about backups for an area, use the command:

ccontroller-1# show atmf backup area

The following figure shows example output from running this command.
Table 45-15: Output from the **show atmf backup area** command

```
controller-1#show atmf backup area

Scheduled Backup ...... Enabled
  Schedule .............. 12 per day starting at 14:30
  Next Backup Time .... 15 Apr 2015 04:30
Backup Bandwidth ...... Unlimited
Backup Media ......... FILE SERVER 1 (Total 128886.5MB, Free 26234.2MB)
Server Config ........
  * 1 .................. Configured   (Mounted, Active)
    Host .............. 10.37.74.1
    Username .......... root
    Path ............... /tftpboot/backups_from_controller-1
    Port ............... -
  2 ................... Configured   (Unmounted)
    Host .............. 10.37.142.1
    Username .......... root
    Path ............... -
    Port ............... -
Current Action ......... Idle
Started ................ -
Current Node ......... -

<table>
<thead>
<tr>
<th>Area Name</th>
<th>Node Name</th>
<th>Id</th>
<th>Date</th>
<th>Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wellington</td>
<td>camry</td>
<td>1</td>
<td>15 Apr 2015</td>
<td>02:30:22</td>
<td>Good</td>
</tr>
<tr>
<td>Canterbury</td>
<td>corona</td>
<td>1</td>
<td>15 Apr 2015</td>
<td>02:30:23</td>
<td>Good</td>
</tr>
<tr>
<td>Canterbury</td>
<td>Avensis</td>
<td>1</td>
<td>15 Apr 2015</td>
<td>02:30:22</td>
<td>Good</td>
</tr>
<tr>
<td>Auckland</td>
<td>RAV4</td>
<td>1</td>
<td>15 Apr 2015</td>
<td>02:30:23</td>
<td>Good</td>
</tr>
<tr>
<td>Southland</td>
<td>MR2</td>
<td>1</td>
<td>15 Apr 2015</td>
<td>02:30:24</td>
<td>Good</td>
</tr>
</tbody>
</table>
```

**Related Commands**

- atmf backup area-masters enable
- show atmf area
- show atmf area nodes-detail
- switchport atmf-arealink remote-area
show atmf detail

**Overview**  
This command displays details about an AMF node. It can only be run on AMF master and controller nodes.

**Syntax**  
show atmf [detail]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Displays output in greater depth.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec

**Example 1**  
To display the AMF node1 information in detail, use the command:

```
controller-1# show atmf detail
```

A typical output screen from this command is shown below:

```
controller-1# show atmf detail
ATMF Detail Information:

Network Name       : Test_network
Node Name          : controller-1
Node Address       : controller-1.atmf
Node ID            : 342
Node Depth         : 0
Domain State       : BackupDomainController
Recovery State     : None
Log Verbose Setting: Verbose

Management VLAN
VLAN ID            : 4000
Management Subnet  : 172.31.0.0
Management IP Address : 172.31.1.86
Management Mask    : 255.255.128.0
Management IPv6 Address : fd00:4154:4d46:1::156
Management IPv6 Prefix Length : 64

Domain VLAN
VLAN ID            : 4091
```

Table 45-16: Parameter definitions from the `show atmf detail` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATMF Status</td>
<td>The Node’s AMF status, either Enabled or Disabled.</td>
</tr>
<tr>
<td>Network Name</td>
<td>The AMF network that a particular node belongs to.</td>
</tr>
<tr>
<td>Node Name</td>
<td>The name assigned to a particular node.</td>
</tr>
</tbody>
</table>
### Table 45-16: Parameter definitions from the `show atmfl detail` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>The role configured for this AMF device, either Master or Member.</td>
</tr>
<tr>
<td>Current ATMF Nodes</td>
<td>The count of AMF nodes in an AMF Network.</td>
</tr>
<tr>
<td>Node Address</td>
<td>An Address used to access a remotely located node. This is simply the Node Name plus the dotted suffix atmfl (.atmf).</td>
</tr>
<tr>
<td>Node ID</td>
<td>A Unique identifier assigned to a Node on an AMF network.</td>
</tr>
<tr>
<td>Node Depth</td>
<td>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.</td>
</tr>
<tr>
<td>Domain State</td>
<td>The state of Node in a Domain in AMF network as Controller/Backup.</td>
</tr>
<tr>
<td>Recovery State</td>
<td>The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.</td>
</tr>
<tr>
<td>Management VLAN</td>
<td>The VLAN created for traffic between Nodes of different domain (up/down links).</td>
</tr>
<tr>
<td>Domain VLAN</td>
<td>The VLAN assigned for traffic between Nodes of same domain (crosslink).</td>
</tr>
<tr>
<td>Device Type</td>
<td>The Product Series Name.</td>
</tr>
<tr>
<td>ATMF Master</td>
<td>'Y' if the node belongs to a Core domain.</td>
</tr>
<tr>
<td>SC</td>
<td>The device configuration, one of C - Chassis (SBx8100 series), S - Stackable (VCS) or N - Standalone.</td>
</tr>
<tr>
<td>Parent</td>
<td>The Node to which the current node has an active uplink.</td>
</tr>
<tr>
<td>Node Depth</td>
<td>The number of nodes in the path from this node to the Core domain.</td>
</tr>
</tbody>
</table>
show atmf group

**Overview**
This command can be used to display the group membership within to a particular AMF node. It can also be used with the working-set command to display group membership within a working set.

Each node in the AMF is automatically added to the group that is appropriate to its hardware architecture, e.g. x510, x610. Nodes that are configured as masters are automatically assigned to the master group.

You can create arbitrary groups of AMF members based on your own selection criteria. You can then assign commands collectively to any of these groups.

**Syntax**
```
show atmf group [user-defined|automatic]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-defined</td>
<td>User-defined-group information display.</td>
</tr>
<tr>
<td>automatic</td>
<td>Automatic group information display.</td>
</tr>
</tbody>
</table>

**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:
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 1939. This can be seen from the network level prompt, which in this case is AMF_NETWORK[6]#.

Table 45-17: Sample output from the show atmf group command for a working set.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATMF group information</td>
<td>Displays a list of nodes and the groups that they belong to, for example:</td>
</tr>
<tr>
<td></td>
<td>• master - Shows a common group name for Nodes configured as AMF masters.</td>
</tr>
<tr>
<td></td>
<td>• Hardware Arch - Shows a group for all Nodes sharing a common Hardware architecture, e.g. x8100, x610, for example.</td>
</tr>
<tr>
<td></td>
<td>• User-defined - Arbitrary groups created by the user for AMF nodes.</td>
</tr>
</tbody>
</table>
show atmf group members

Overview  This command will display all group memberships within an AMF working-set. Each node in the AMF working set is automatically added to automatic groups which are defined by hardware architecture, e.g. x510, x610. Nodes that are configured as masters are automatically assigned to the master group. Users can define arbitrary groupings of AMF members based on their own criteria, which can be used to select groups of nodes.

Syntax  show atmf group members [user-defined|automatic]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-defined</td>
<td>User defined group membership display.</td>
</tr>
<tr>
<td>automatic</td>
<td>Automatic group membership display.</td>
</tr>
</tbody>
</table>

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 45-19: Sample output from the `show atmf group members` command

<table>
<thead>
<tr>
<th>ATMF Group membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Groups</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>master</td>
</tr>
<tr>
<td>poe</td>
</tr>
<tr>
<td>x510</td>
</tr>
<tr>
<td>x610</td>
</tr>
<tr>
<td>x8100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ATMF Group membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-defined Groups</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>marketing</td>
</tr>
<tr>
<td>software</td>
</tr>
</tbody>
</table>
Table 45-20: Parameter definitions from the `show atmf group members` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Groups</td>
<td>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.</td>
</tr>
<tr>
<td>User-defined Groups</td>
<td>Shows the grouping of AMF nodes in user defined groups.</td>
</tr>
<tr>
<td>Total Members</td>
<td>Shows the total number of members in each group.</td>
</tr>
<tr>
<td>Members</td>
<td>Shows the list of AMF nodes in each group.</td>
</tr>
</tbody>
</table>
**show atmf links**

**Overview**
This command displays brief information about AMF links on a device, such as link status and adjacent nodes.

Provisioned node names will be displayed with a trailing * character, and will not have an entry under Adjacent Ifindex.

This command can only be run on AMF master and controller nodes.

**Syntax**
show atmf links

**Mode**
User Exec and Privileged Exec

**Example**
To display the AMF links brief details, use the following command:

```
controller-1# show atmf links brief
```

Figure 45-8: Sample output from the show atmf links command

```
device1# show atmf link brief
ATMF Links Brief:

<table>
<thead>
<tr>
<th>Local</th>
<th>Link</th>
<th>Port</th>
<th>ATMF</th>
<th>Adjacent</th>
<th>Adjacent Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>sal</td>
<td>Crosslink Up</td>
<td>TwoWay</td>
<td>Building_1</td>
<td>4501</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1.0.1</td>
<td>Downlink Up</td>
<td>Full</td>
<td>Bld1_Floor_1</td>
<td>5001</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1.0.2</td>
<td>Downlink Up</td>
<td>Full</td>
<td>Bld1_Floor_2</td>
<td>5003</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1.0.3</td>
<td>Downlink Up</td>
<td>Full</td>
<td>Bld2_Floor_1</td>
<td>6101</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1.0.4</td>
<td>Crosslink Down</td>
<td>Init</td>
<td>*device3</td>
<td>Blocking</td>
<td></td>
</tr>
</tbody>
</table>

* = provisioned
```

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Related Commands**
- no debug all
- clear atmf links statistics
- show atmf
- show atmf nodes
show atmf links detail

**Overview**
This command displays detailed information on all the links configured in the AMF network. It can only be run on AMF master and controller nodes.

**Syntax**
show atmf links [detail]

**Mode**
User Exec

**Example**
To display the AMF link details use this command:

```
device1# show atmf links detail
```

The output from this command will display all the internal data held for AMF links.

Table 45-21: Sample output from the **show atmf links detail** command

```
device1# show atmf links details

ATMF Links Detail:

Port : sa1
Ifindex : 4501
VR ID : 0
Port Status : Up
Port State : Full
Port BPDU Receive Count : 44441
Adjacent Node Name : Building_2
Adjacent Ifindex : 4501
Adjacent VR ID : 0
Adjacent MAC : 0014.2299.137d
Port Last Message Response : 0
```
### Table 45-21: Sample output from the `show atmf links detail` command (cont.)

<table>
<thead>
<tr>
<th>Port</th>
<th>: port2.0.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ifindex</td>
<td>: 6002</td>
</tr>
<tr>
<td>VR ID</td>
<td>: 0</td>
</tr>
<tr>
<td>Port Status</td>
<td>: Down</td>
</tr>
<tr>
<td>Port State</td>
<td>: Init</td>
</tr>
<tr>
<td>Port BPDU Receive Count</td>
<td>: 0</td>
</tr>
</tbody>
</table>

**Link State Entries:**

- **Node.Ifindex**: Building_2.4501 -
- **Building_1.4501 Transaction ID**: 3 - 3
- **MAC Address**: 0014.2299.137d - eccd.6d03.10e3
- **Link State**: Full - Full

**Domain Nodes Tree:**

- **Node**: Building_2
  - **Links on Node**: 1
  - **Link 0**: Building_2.4501 -
  - **Building_1.4501 Forwarding State**: Forwarding

- **Node**: Building_1
  - **Links on Node**: 1
  - **Link 0**: Building_2.4501 -
  - **Building_1.4501 Forwarding State**: Forwarding

**Crosslink Transaction Entries:**

- **Node**: Building_2
  - **Transaction ID**: 3
  - **Uplink Transaction ID**: 3
  - **Uplink Information:**
    - **Waiting for Sync**: 0
    - **Transaction ID**: 3
    - **Number of Links**: 0
    - **Number of Local Uplinks**: 0

**Uplink Information:**

- **Waiting for Sync**: 0
- **Transaction ID**: 3
- **Number of Links**: 0
- **Number of Local Uplinks**: 0
- **Originating Node**: Building_2
- **Domain**: -’s domain
- **Node**: Building_2
- **Ifindex**: 0
- **VR ID**: 0
- **Transaction ID**: 3
- **Flags**: 32
- **Domain Controller**: -
- **Domain Controller MAC**: 0000.0000.0000
Table 45-21: Sample output from the `show atmf links detail` command (cont.)

<table>
<thead>
<tr>
<th>Downlink Domain Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain                       : Bld2_Floor_1's domain</td>
</tr>
<tr>
<td>Domain Controller            : Bld2_Floor_1</td>
</tr>
<tr>
<td>Domain Controller MAC        : eccd.6d3f.fef7</td>
</tr>
<tr>
<td>Number of Links              : 2</td>
</tr>
<tr>
<td>Number of Links Up           : 2</td>
</tr>
<tr>
<td>Number of Links on This Node : 1</td>
</tr>
<tr>
<td>Links are Blocked            : 0</td>
</tr>
<tr>
<td>Node Transaction List        :</td>
</tr>
<tr>
<td>Node                         : Building_2</td>
</tr>
<tr>
<td>Transaction ID               : 7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain                       : Bld2_Floor_1's domain</td>
</tr>
<tr>
<td>Node                         : Building_2</td>
</tr>
<tr>
<td>Ifindex                      : 5002</td>
</tr>
<tr>
<td>Transaction ID               : 7</td>
</tr>
<tr>
<td>Flags                        : 1</td>
</tr>
</tbody>
</table>

| Domain                       : Bld2_Floor_1's domain |
| Node                         : Building_1 |
| Ifindex                      : 7002 |
| Transaction ID               : 7 |
| Flags                        : 1 |

<table>
<thead>
<tr>
<th>Up/Downlink Ports Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port                           : port1.3.1</td>
</tr>
<tr>
<td>Ifindex                        : 7001</td>
</tr>
<tr>
<td>VR ID                          : 0</td>
</tr>
<tr>
<td>Port Status                    : Up</td>
</tr>
<tr>
<td>Port State                     : Full</td>
</tr>
<tr>
<td>Adjacent Node                  : Bld1_Floor_1</td>
</tr>
<tr>
<td>Adjacent Internal ID           : 4</td>
</tr>
<tr>
<td>Adjacent Ifindex               : 6001</td>
</tr>
<tr>
<td>Adjacent Board ID              : 290</td>
</tr>
<tr>
<td>Adjacent VR ID                 : 0</td>
</tr>
<tr>
<td>Adjacent MAC                   : 0000.cd37.0ea4</td>
</tr>
<tr>
<td>Adjacent Domain Controller     : Bld1_Floor_1</td>
</tr>
<tr>
<td>Adjacent Domain Controller MAC : 0000.cd37.0ea4</td>
</tr>
<tr>
<td>Port Forwarding State          : Blocking</td>
</tr>
<tr>
<td>Port BPDU Receive Count        : 0</td>
</tr>
<tr>
<td>Port Sequence Number           : 12</td>
</tr>
<tr>
<td>Port Adjacent Sequence Number  : 9</td>
</tr>
<tr>
<td>Port Last Message Response     : 0</td>
</tr>
</tbody>
</table>
Table 45-21: Sample output from the `show atmf links detail` command (cont.)

<table>
<thead>
<tr>
<th>Port</th>
<th>: port1.3.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ifindex</td>
<td>: 7002</td>
</tr>
<tr>
<td>VR ID</td>
<td>: 0</td>
</tr>
<tr>
<td>Port Status</td>
<td>: Up</td>
</tr>
<tr>
<td>Port State</td>
<td>: Full</td>
</tr>
<tr>
<td>Adjacent Node</td>
<td>: Bld2_Floor_1</td>
</tr>
<tr>
<td>Adjacent Internal ID</td>
<td>: 3</td>
</tr>
<tr>
<td>Adjacent Ifindex</td>
<td>: 5001</td>
</tr>
<tr>
<td>Adjacent Board ID</td>
<td>: 333</td>
</tr>
<tr>
<td>Adjacent VR ID</td>
<td>: 0</td>
</tr>
<tr>
<td>Adjacent MAC</td>
<td>: eccd.6d3f.fef7</td>
</tr>
<tr>
<td>Adjacent Domain Controller</td>
<td>: Bld2_Floor_1</td>
</tr>
<tr>
<td>Adjacent Domain Controller MAC</td>
<td>: eccd.6d3f.fef7</td>
</tr>
<tr>
<td>Port Forwarding State</td>
<td>: Blocking</td>
</tr>
<tr>
<td>Port BPDU Receive Count</td>
<td>: 0</td>
</tr>
<tr>
<td>Port Sequence Number</td>
<td>: 15</td>
</tr>
<tr>
<td>Port Adjacent Sequence Number</td>
<td>: 8</td>
</tr>
<tr>
<td>Port Last Message Response</td>
<td>: 0</td>
</tr>
</tbody>
</table>

Table 45-22: Parameter definitions from the `show atmf links detail` command output

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Status</td>
<td>Shows status of the local port on the Node as UP/DOWN.</td>
</tr>
<tr>
<td>Adjacent Node</td>
<td>Shows Adjacent AMF Node to this Node.</td>
</tr>
<tr>
<td>Adjacent IfIndex</td>
<td>Shows interface on the Adjacent AMF Node connected to this Node.</td>
</tr>
<tr>
<td>Link State</td>
<td>Shows state of AMF link Forwarding/Blocking.</td>
</tr>
<tr>
<td>Crosslink Ports Information</td>
<td>Show details of all Crosslink ports on this Node:</td>
</tr>
<tr>
<td></td>
<td>Port - Name of the Port or static aggregation (sa&lt;*&gt;).</td>
</tr>
<tr>
<td></td>
<td>Ifindex - Interface index for the crosslink port.</td>
</tr>
<tr>
<td></td>
<td>VR ID - Virtual router id for the crosslink port.</td>
</tr>
<tr>
<td></td>
<td>Port Status - Shows status of the local port on the Node as UP/DOWN.</td>
</tr>
<tr>
<td></td>
<td>Port State - Same as AMF state as described above.</td>
</tr>
<tr>
<td></td>
<td>Port BPDU Receive Count - The number of AMF protocol PDU's received.</td>
</tr>
<tr>
<td></td>
<td>Adjacent Node Name - name of the adjacent node in the domain.</td>
</tr>
<tr>
<td></td>
<td>Adjacent Ifindex - Ifindex of the adjacent node in the domain.</td>
</tr>
<tr>
<td></td>
<td>Adjacent VR ID - Virtual router id of the adjacent node in the domain.</td>
</tr>
<tr>
<td></td>
<td>Adjacent MAC - MAC address of the adjacent node in the domain.</td>
</tr>
<tr>
<td></td>
<td>Port Last Message Response - Response from the remote neighbor to our</td>
</tr>
<tr>
<td></td>
<td>AMF last hello packet.</td>
</tr>
<tr>
<td>Link State Entries</td>
<td>Show all the link state database entries:</td>
</tr>
<tr>
<td></td>
<td>Node.Ifindex - Shows adjacent Node names and Interface index.</td>
</tr>
<tr>
<td></td>
<td>Transaction ID - Shows transaction id of the current crosslink transaction.</td>
</tr>
<tr>
<td></td>
<td>MAC Address - Shows adjacent Node MAC addresses.</td>
</tr>
<tr>
<td></td>
<td>Link State - Shows AMF states of adjacent nodes on the link.</td>
</tr>
</tbody>
</table>
### Table 45-22: Parameter definitions from the `show atmf links detail` command output (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain Nodes Tree</strong></td>
<td>Shows all the nodes in the domain:</td>
</tr>
<tr>
<td></td>
<td>- Node - Name of the node in the domain.</td>
</tr>
<tr>
<td></td>
<td>- Links on Node - Number of crosslinks on a vertex/node.</td>
</tr>
<tr>
<td></td>
<td>- Link no - Shows adjacent Node names and Interface index.</td>
</tr>
<tr>
<td></td>
<td>- Forwarding State - Shows state of AMF link Forwarding/Blocking.</td>
</tr>
<tr>
<td><strong>Crosslink Transaction Entries</strong></td>
<td>Shows all the transaction entries:</td>
</tr>
<tr>
<td></td>
<td>- Node - Name of the AMF node.</td>
</tr>
<tr>
<td></td>
<td>- Transaction ID - transaction id of the node.</td>
</tr>
<tr>
<td></td>
<td>- Uplink Transaction ID - transaction id of the remote node.</td>
</tr>
<tr>
<td><strong>Uplink Information</strong></td>
<td>Show all uplink entries.</td>
</tr>
<tr>
<td></td>
<td>- Waiting for Sync - Flag if uplinks are currently waiting for synchronization.</td>
</tr>
<tr>
<td></td>
<td>- Transaction ID - Shows transaction id of the local node.</td>
</tr>
<tr>
<td></td>
<td>- Number of Links - Number of up downlinks in the domain.</td>
</tr>
<tr>
<td></td>
<td>- Number of Local Uplinks - Number of uplinks on this node to the parent domain.</td>
</tr>
<tr>
<td></td>
<td>- Originating Node - Node originating the uplink information.</td>
</tr>
<tr>
<td></td>
<td>- Domain - Name of the parent uplink domain.</td>
</tr>
<tr>
<td></td>
<td>- Node - Name of the node in the parent domain, that is connected to the current domain.</td>
</tr>
<tr>
<td></td>
<td>- Ifindex - Interface index of the parent node’s link to the current domain.</td>
</tr>
<tr>
<td></td>
<td>- VR ID - Virtual router id of the parent node’s link to the current domain.</td>
</tr>
<tr>
<td></td>
<td>- Transaction ID - Transaction identifier for the neighbor in crosslink.</td>
</tr>
<tr>
<td></td>
<td>- Flags - Used in domain messages to exchange the state:</td>
</tr>
<tr>
<td></td>
<td>- ATMF_DOMAIN_FLAG_DOWN = 0</td>
</tr>
<tr>
<td></td>
<td>- ATMF_DOMAIN_FLAG_UP = 1</td>
</tr>
<tr>
<td></td>
<td>- ATMF_DOMAIN_FLAG_BLOCK = 2</td>
</tr>
<tr>
<td></td>
<td>- ATMF_DOMAIN_FLAG_NOT_PRESENT = 4</td>
</tr>
<tr>
<td></td>
<td>- ATMF_DOMAIN_FLAG_NO_NODE = 8</td>
</tr>
<tr>
<td></td>
<td>- ATMF_DOMAIN_FLAG_NOT_ACTIVE_PARENT = 16</td>
</tr>
<tr>
<td></td>
<td>- ATMF_DOMAIN_FLAG_NO_LINKS = 32</td>
</tr>
<tr>
<td></td>
<td>- ATMF_DOMAIN_FLAG_NO_CONFIG = 64</td>
</tr>
<tr>
<td></td>
<td>- Domain Controller - Domain Controller in the uplink domain</td>
</tr>
<tr>
<td></td>
<td>- Domain Controller MAC - MAC address of Domain Controller in uplink domain</td>
</tr>
</tbody>
</table>
Table 45-22: Parameter definitions from the **show atmf links detail** command output (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Domain Information</td>
<td>Shows all the downlink entries:</td>
</tr>
<tr>
<td></td>
<td>● Domain - Name of the downlink domain.</td>
</tr>
<tr>
<td></td>
<td>● Domain Controller - Controller of the downlink domain.</td>
</tr>
<tr>
<td></td>
<td>● Domain Controller MAC - MAC address of the domain controller.</td>
</tr>
<tr>
<td></td>
<td>● Number of Links - Total number of links to this domain from the Node.</td>
</tr>
<tr>
<td></td>
<td>● Number of Links Up - Total number of links that are in UP state.</td>
</tr>
<tr>
<td></td>
<td>● Number of Links on This Node - Number of links terminating on this node.</td>
</tr>
<tr>
<td></td>
<td>● Links are Blocked - 0 links are not blocked to the domain. 1 All links are blocked to the domain.</td>
</tr>
</tbody>
</table>
### Node Transaction List

- **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

- **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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.
**Related Commands**

- no debug all
- clear atmf links statistics
- show atmf
show atmf links statistics

**Overview**  This command displays details of the AMF links configured on the device and also displays statistics about the AMF packet exchanges between the devices.

It is also possible to display the AMF link configuration and packet exchange statistics for a specified interface.

This command can only be run on AMF master and controller nodes

**Syntax**  show atmf links statistics [interface [<port_number>]]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;port_number&gt;</td>
<td>Enter the port number for which statistics are required. A port range or a static channel can also be specified. Where no port number is specified, statistics will be displayed for all ports on the device.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec

**Example 1**  To display AMF link statistics for the whole device, use the command:

device1# show atmf links statistics
Table 45-23: Sample output from the `show atmf links statistics` command

```
device1# show atmf links statistics

ATMF Statistics:

<table>
<thead>
<tr>
<th></th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arealink Hello</td>
<td>124082</td>
<td>124052</td>
</tr>
<tr>
<td>Crosslink Hello</td>
<td>20665</td>
<td>20666</td>
</tr>
<tr>
<td>Crosslink Hello Domain</td>
<td>10336</td>
<td>10338</td>
</tr>
<tr>
<td>Crosslink Hello Uplink</td>
<td>10333</td>
<td>10338</td>
</tr>
<tr>
<td>Hello Link</td>
<td>41313</td>
<td>82649</td>
</tr>
<tr>
<td>Hello Neighbor</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Hello Stack</td>
<td>82652</td>
<td>82659</td>
</tr>
<tr>
<td>Hello Gateway</td>
<td>165168</td>
<td>165281</td>
</tr>
<tr>
<td>Database Description</td>
<td>42</td>
<td>43</td>
</tr>
<tr>
<td>Database Request</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>Database Update</td>
<td>2885</td>
<td>5496</td>
</tr>
<tr>
<td>Database Update Bitmap</td>
<td>0</td>
<td>115</td>
</tr>
<tr>
<td>Database Acknowledge</td>
<td>5331</td>
<td>2746</td>
</tr>
<tr>
<td>Transmit Fails</td>
<td>0</td>
<td>38</td>
</tr>
<tr>
<td>Discards</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>Total ATMF Packets</td>
<td>462823</td>
<td>504386</td>
</tr>
</tbody>
</table>

ATMF Database Statistics:

Database Entries: 15
Database Full Ages: 2

ATMF Packet Discards:

<table>
<thead>
<tr>
<th>Type</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type0</td>
<td>0</td>
<td>Type1</td>
</tr>
<tr>
<td>Type1</td>
<td>0</td>
<td>Type2</td>
</tr>
<tr>
<td>Type2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Type3</td>
<td>0</td>
<td>Type4</td>
</tr>
<tr>
<td>Type4</td>
<td>0</td>
<td>Type5</td>
</tr>
<tr>
<td>Type5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Type6</td>
<td>0</td>
<td>Type7</td>
</tr>
<tr>
<td>Type7</td>
<td>0</td>
<td>Type8</td>
</tr>
<tr>
<td>Type8</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Type9</td>
<td>0</td>
<td>Type10</td>
</tr>
<tr>
<td>Type10</td>
<td>0</td>
<td>Type11</td>
</tr>
<tr>
<td>Type11</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Type12</td>
<td>0</td>
<td>Type13</td>
</tr>
<tr>
<td>Type13</td>
<td>0</td>
<td>Type14</td>
</tr>
<tr>
<td>Type14</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Type15</td>
<td>0</td>
<td>Type16</td>
</tr>
<tr>
<td>Type16</td>
<td>0</td>
<td>Type17</td>
</tr>
<tr>
<td>Type17</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Type18</td>
<td>0</td>
<td>Type19</td>
</tr>
<tr>
<td>Type19</td>
<td>0</td>
<td>Type20</td>
</tr>
<tr>
<td>Type20</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Type21</td>
<td>0</td>
<td>Type22</td>
</tr>
<tr>
<td>Type22</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

ATMF Virtual Link Statistics

<table>
<thead>
<tr>
<th>Virtual Link</th>
<th>Receive</th>
<th>Dropped</th>
<th>Transmit</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlink3</td>
<td>97383</td>
<td>0</td>
<td>36260</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Example 2**

To display the AMF links statistics on interface port1.0.5, use the command:

```
device1# show atmf links statistics interface port1.0.5
```
Figure 45-9: Sample output from the `show atmf links statistics` command for interface 1.0.5

```
device1# show atmf links statistics interface port1.0.5
ATMF Port Statistics:

<table>
<thead>
<tr>
<th>Transmit</th>
<th>Receive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crosslink Hello</td>
<td>231</td>
</tr>
<tr>
<td>Crosslink Hello Domain</td>
<td>116</td>
</tr>
<tr>
<td>Crosslink Hello Uplink</td>
<td>116</td>
</tr>
<tr>
<td>Hello Link</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Figure 45-10: Parameter definitions from the `show atmf links statistics` command output

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive</td>
<td>Shows a count of AMF protocol packets received per message type.</td>
</tr>
<tr>
<td>Transmit</td>
<td>Shows the number of AMF protocol packets transmitted per message type.</td>
</tr>
<tr>
<td>Database Entries</td>
<td>Shows the number of AMF elements existing in the distributed database.</td>
</tr>
</tbody>
</table>
### AMF Commands

**SHOW ATMF LINKS STATISTICS**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database Full Ages</strong></td>
<td>Shows the number of times the entries aged in the database.</td>
</tr>
</tbody>
</table>
| **ATMF Packet Discards** | Shows the number of discarded packets of each type:  
  - Type0: The number of discarded crosslink hello msgs received on a non crosslink port.  
  - Type1: The number of discarded tx update packets - bad checksum.  
  - Type2: The number of discarded tx update bitmap packets - bad checksum.  
  - Type3: The number of discarded tx update packets - neighbor not in the correct state.  
  - Type4: The number of discarded update packets - bad checksum.  
  - Type5: The number of discarded update packets - neighbor not in the correct state.  
  - Type6: The number of discarded update bitmap packets - bad checksum.  
  - Type7: The number of discarded crosslink hello msgs received on a non crosslink port.  
  - Type8: The number of discarded crosslink hello msg received on a port that is not in the correct state.  
  - Type9: The number of discarded crosslink domain hello msgs received on a non crosslink port.  
  - Type10: The number of discarded crosslink domain hello msgs received on a port that is not in the correct state.  
  - Type11: The number of crosslink uplink hello msgs received on a non crosslink port.  
  - Type12: The number of discarded crosslink uplink hello msgs ignored on a port that is not in the correct state.  
  - Type13: The number of messages with an incorrect name for this AMF network.  
  - Type14: The number of over-long packets received on a port.  
  - Type15: The number of messages with a bad protocol version received on a port.  
  - Type16: The number of messages with a bad packet checksum calculation received on a port.  
  - Type17: The number of messages with a bad authentication type received on a port.  
  - Type18: The number of messages with a bad simple password received on a port.  
  - Type19: The number of discarded packets with an unsupported authentication type received on a port.  
  - Type20: The number of discarded packets with an unknown neighbor received on a port. |

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.
Related Commands

- no debug all
- clear atmf links statistics
- show atmf
show atmf memory

**Overview**  
This command displays a summary of the AMF memory usage. It can only be run on AMF master nodes.

**Syntax**  
`show atmf memory`

**Mode**  
User Exec

**Example**  
To display AMF memory allocations on Node_1, use the command:

```
node_1# show atmf memory
```

Table 45-24: Sample output from the `show atmf memory` command

<table>
<thead>
<tr>
<th>Line</th>
<th>Number</th>
<th>Memory</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1238</td>
<td>1</td>
<td>memory</td>
<td>28</td>
</tr>
<tr>
<td>244</td>
<td>2</td>
<td>memory</td>
<td>88</td>
</tr>
<tr>
<td>3753</td>
<td>2</td>
<td>memory</td>
<td>1872</td>
</tr>
<tr>
<td>1616</td>
<td>8</td>
<td>memory</td>
<td>320</td>
</tr>
<tr>
<td>1391</td>
<td>1</td>
<td>memory</td>
<td>60</td>
</tr>
<tr>
<td>1837</td>
<td>15</td>
<td>memory</td>
<td>600</td>
</tr>
<tr>
<td>288</td>
<td>1</td>
<td>memory</td>
<td>28716</td>
</tr>
<tr>
<td>3916</td>
<td>1</td>
<td>memory</td>
<td>1520</td>
</tr>
<tr>
<td>1623</td>
<td>0</td>
<td>memory</td>
<td>320</td>
</tr>
<tr>
<td>4477</td>
<td>1</td>
<td>memory</td>
<td>1520</td>
</tr>
<tr>
<td>659</td>
<td>2</td>
<td>memory</td>
<td>512</td>
</tr>
<tr>
<td>1844</td>
<td>6</td>
<td>memory</td>
<td>600</td>
</tr>
<tr>
<td>1749</td>
<td>1</td>
<td>memory</td>
<td>32</td>
</tr>
<tr>
<td>203</td>
<td>6</td>
<td>memory</td>
<td>600</td>
</tr>
<tr>
<td>4205</td>
<td>1</td>
<td>memory</td>
<td>1520</td>
</tr>
<tr>
<td>206</td>
<td>4</td>
<td>memory</td>
<td>1524</td>
</tr>
<tr>
<td>549</td>
<td>1</td>
<td>memory</td>
<td>232</td>
</tr>
<tr>
<td>3495</td>
<td>1</td>
<td>memory</td>
<td>56</td>
</tr>
<tr>
<td>2628</td>
<td>2</td>
<td>memory</td>
<td>72</td>
</tr>
<tr>
<td>678</td>
<td>1</td>
<td>memory</td>
<td>32</td>
</tr>
<tr>
<td>1423</td>
<td>1</td>
<td>memory</td>
<td>48</td>
</tr>
<tr>
<td>1733</td>
<td>3</td>
<td>memory</td>
<td>492</td>
</tr>
<tr>
<td>1611</td>
<td>8</td>
<td>memory</td>
<td>256</td>
</tr>
</tbody>
</table>
### Table 45-24: Sample output from the `show atmf memory` command (cont.)

<table>
<thead>
<tr>
<th>ATMF Memory Deallocation:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total memory deallocated  : 4958 (bytes)</td>
</tr>
<tr>
<td>Total memory deallocations : 45</td>
</tr>
<tr>
<td>Line 1395 number 4 memory 400 (bytes)</td>
</tr>
<tr>
<td>Line 1956 number 1 memory 164 (bytes)</td>
</tr>
<tr>
<td>Line 1247 number 1 memory 52 (bytes)</td>
</tr>
<tr>
<td>Line 876 number 2 memory 80 (bytes)</td>
</tr>
<tr>
<td>Line 166 number 1 memory 232 (bytes)</td>
</tr>
<tr>
<td>Line 415 number 7 memory 587 (bytes)</td>
</tr>
<tr>
<td>Line 418 number 3 memory 300 (bytes)</td>
</tr>
<tr>
<td>Line 822 number 2 memory 80 (bytes)</td>
</tr>
<tr>
<td>Line 2341 number 4 memory 160 (bytes)</td>
</tr>
<tr>
<td>Line 3025 number 2 memory 88 (bytes)</td>
</tr>
<tr>
<td>Line 144 number 3 memory 1596 (bytes)</td>
</tr>
<tr>
<td>Line 146 number 6 memory 312 (bytes)</td>
</tr>
<tr>
<td>Line 2349 number 4 memory 160 (bytes)</td>
</tr>
<tr>
<td>Line 1111 number 1 memory 59 (bytes)</td>
</tr>
<tr>
<td>Line 1393 number 4 memory 688 (bytes)</td>
</tr>
</tbody>
</table>

```
------------------------------------------------------
Total memory in use        : 4958 (bytes)
Total memory items         : 45
```
show atmf nodes

**Overview**  This command displays all nodes currently configured within the AMF network. It displays a topographical representation of the network infrastructure.

This command displays a summary of all virtual links currently in the running configuration.

**Syntax**  show atmf nodes

**Mode**  Privileged Exec

**Example**  To display AMF information for all nodes in the AMF, use the command:

```plaintext
node_1# show atmf nodes
```

Table 45-25: Sample output from the `show atmf nodes` command.

```
nodel#show atmf nodes

Node Information:
 * = Local device

SC = Switch Configuration:
 C = Chassis   S = Stackable   N = Standalone

<table>
<thead>
<tr>
<th>Node Name</th>
<th>Device</th>
<th>ATMF Master</th>
<th>SC</th>
<th>Parent</th>
<th>Node Depth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building_1</td>
<td>AT-SBx8112</td>
<td>Y</td>
<td>C</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>* Bld1_Floor_1</td>
<td>SwitchBlade x908</td>
<td>N</td>
<td>S</td>
<td>Building_1</td>
<td>1</td>
</tr>
<tr>
<td>Bld1_Floor_2</td>
<td>x600-24Ts/XP</td>
<td>N</td>
<td>N</td>
<td>Building_1</td>
<td>1</td>
</tr>
<tr>
<td>Bld2_Floor_1</td>
<td>x610-24Ts-POE+</td>
<td>N</td>
<td>N</td>
<td>Building_1</td>
<td>1</td>
</tr>
<tr>
<td>SW_Team1</td>
<td>x210-24GT</td>
<td>N</td>
<td>N</td>
<td>Bld1_Floor_2</td>
<td>2</td>
</tr>
</tbody>
</table>

Current ATMF node count 6
```
show atmf provision nodes

Overview
This command displays information about each provisioned node with details about date and time of creation, boot and configuration files available in the backup, and license files present in the provisioned backup. This includes nodes that have joined the network but are yet to run their first backup.

This command can only be run on AMF master and controller nodes.

Syntax
show atmf provision nodes

Mode
Privileged Exec

Usage
This command will only work if provisioned nodes have already been set up. Otherwise, an error message is shown when the command is run.

Example
To show the details of all the provisioned nodes in the backup use the command:

```
NodeName# show atmf provision nodes
```

Figure 45-11: Sample output from the `show atmf provision nodes` command

```
device1# show atmf provision nodes

ATMF Provisioned Node Information:
Backup Media .............: SD (Total 3827.0MB, Free 3481.1MB)
Node Name ...............: device2
Date & Time .............: 06-May-2014 & 23:25:44
Provision Path ..........: card:/atmf/provision_nodes

Boot configuration :
Current boot image ....: x510-1766_atmf_backup.rel (file exists)
Backup boot image .....: x510-main-20140113-2.rel (file exists)
Default boot config ...: flash:/default.cfg (file exists)
Current boot config ...: flash:/abc.cfg (file exists)
Backup boot config ...: flash:/xyz.cfg (file exists)

Software Licenses :
Repository file ........: ~/.configs/.sw_v2.lic
Certificate file ......: card:/atmf/nodes/awplus1/flash/.atmf-lic-cert
```

Related commands
- `atmf provision node create`
- `atmf provision node clone`
- `atmf provision node configure boot config`
- `atmf provision node configure boot system`
- `show atmf backup`
show atmf tech

**Overview**  
This command collects and displays all the AMF command output. The command can thus be used to display a complete picture of an AMF network.

**Syntax**  
show atmf tech

**Mode**  
Privileged Exec

**Example**  
To display output for all AMF commands, use the command:

NodeName# show atmf tech

Table 45-26: Sample output from the **show atmf tech** command.

```plaintext
node1# show atmf tech
ATMF Summary Information:
  ATMF Status : Enabled
  Network Name : ATMF_NET
  Node Name : node1
  Role : Master
  Current ATMF Nodes : 8

ATMF Technical information:
  Network Name : ATMF_NET
  Domain : node1's domain
  Node Depth : 0
  Domain Flags : 0
  Authentication Type : 0
  MAC Address : 0014.2299.137d
  Board ID : 287
  Domain State : DomainController
  Domain Controller : node1
  Backup Domain Controller : node2
  Domain controller MAC : 0014.2299.137d
  Parent Domain : -
  Parent Domain Controller : -
  Parent Domain Controller MAC : 0000.0000.0000
  Number of Domain Events : 0
  Crosslink Ports Blocking : 0
  Uplink Ports Waiting on Sync : 0
  Crosslink Sequence Number : 7
  Domains Sequence Number : 28
  Uplink Sequence Number : 2
  Number of Crosslink Ports : 1
  Number of Domain Nodes : 2
  Number of Neighbors : 5
  Number of Non Broadcast Neighbors : 3
  Number of Link State Entries : 1
  Number of Up Uplinks : 0
  Number of Up Uplinks on This Node : 0
  DBE Checksum : 84fc6
  Number of DBE Entries : 0
...
```
Table 45-27: Parameter definitions from the **show atmf tech** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATMF Status</td>
<td>Shows status of AMF feature on the Node as Enabled/Disabled.</td>
</tr>
<tr>
<td>Network Name</td>
<td>The name of the AMF network to which this node belongs.</td>
</tr>
<tr>
<td>Node Name</td>
<td>The name assigned to the node within the AMF network.</td>
</tr>
<tr>
<td>Role</td>
<td>The role configured on the device within the AMF - either master or member.</td>
</tr>
<tr>
<td>Current ATMF Nodes</td>
<td>A count of the AMF nodes in the AMF network.</td>
</tr>
<tr>
<td>Node Address</td>
<td>The identity of a node (in the format name.atmf) that enables its access it from a remote location.</td>
</tr>
<tr>
<td>Node ID</td>
<td>A unique identifier assigned to an AMF node.</td>
</tr>
<tr>
<td>Node Depth</td>
<td>The number of nodes in path from this node to the core domain.</td>
</tr>
<tr>
<td>Domain State</td>
<td>A node's state within an AMF Domain - either controller or backup.</td>
</tr>
<tr>
<td>Recovery State</td>
<td>The AMF node recovery status. Indicates whether a node recovery is in progress on this device - either Auto, Manual, or None.</td>
</tr>
<tr>
<td>Management VLAN</td>
<td>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)</td>
</tr>
<tr>
<td>Domain VLAN</td>
<td>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)</td>
</tr>
<tr>
<td>Device Type</td>
<td>Shows the Product Series Name.</td>
</tr>
<tr>
<td>ATMF Master</td>
<td>Indicates the nodes membership of the core domain (membership is indicated by Y)</td>
</tr>
<tr>
<td>SC</td>
<td>Shows switch configuration:</td>
</tr>
<tr>
<td></td>
<td>• C - Chassis (such as SBx8100 series)</td>
</tr>
<tr>
<td></td>
<td>• S - Stackable (VCS)</td>
</tr>
<tr>
<td></td>
<td>• N - Standalone</td>
</tr>
</tbody>
</table>
Table 45-27: Parameter definitions from the `show atmf tech` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent</td>
<td>A node to which connects to the present node's uplink, i.e. one layer higher in the hierarchy.</td>
</tr>
<tr>
<td>Node Depth</td>
<td>Shows the number of nodes in path from the current node to the Core domain.</td>
</tr>
</tbody>
</table>

**NOTE:** The `show atmf tech` command can produce very large output. For this reason only the most significant terms are defined in this table.
**show atmf working-set**

**Overview**  
This command displays the nodes that form the current AMF working-set.

**Syntax**  
`show atmf working-set`

**Mode**  
Privileged Exec

**Example**  
To show current members of the working-set, use the command:

```
ATMF_NETWORK[6]# show atmf working-set
```

<table>
<thead>
<tr>
<th>ATMF Working Set Nodes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1, node2, node3, node4, node5, node6</td>
</tr>
</tbody>
</table>

**Working set contains 6 nodes**

**Related Commands**

- atmf working-set
- show atmf
- show atmf group
show debugging atmf

**Overview**  This command shows the debugging modes status for AMF.

**Syntax**  show debugging atmf

**Mode**  User Exec and Global Configuration

**Example**  To display the AMF debugging status, use the command:

```
node_1# show debugging atmf
```

Figure 45-12: Sample output from the `show debugging atmf` command.

```
nodel# show debugging atmf
ATMF debugging status:
ATMF arealink debugging is on
ATMF link debugging is on
ATMF crosslink debugging is on
ATMF database debugging is on
ATMF neighbor debugging is on
ATMF packet debugging is on
ATMF error debugging is on
```

**Related Commands**  debug atmf packet
show debugging atmf packet

**Overview**  This command shows details of AMF Packet debug command settings.

**Syntax**  
```
show debugging atmf packet
```

**Mode**  User Exec and Global Configuration

**Example**  To display the AMF packet debugging status, use the command:
```
node_1# show debug atmf packet
```

Figure 45-13: Sample output from the `show debugging atmf packet` command.

```
ATMF packet debugging is on  
=== ATMF Packet Debugging Parameters===  
Node Name: x908  
Port name: port1.1.1  
Limit: 500 packets  
Direction: TX  
Info Level: Level 2  
Packet Type Bitmap:  
  2. Crosslink Hello BPDU pkt with downlink domain info  
  3. Crosslink Hello BPDU pkt with uplink info  
  4. Down and up link Hello BPDU pkts  
  6. Stack hello unicast pkts  
  8. DBE request  
  9. DBE update  
  10. DBE bitmap update
```

**Related Commands**  
- `debug atmf`
- `debug atmf packet`
show running-config atmf

**Overview**  
This command displays the running system information that is specific to AMF.

**Syntax**  
show running-config atmf

**Mode**  
User Exec and Global Configuration

**Example**  
To display the current configuration of AMF, use the following commands:

```
node_1# show running-config atmf
```

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Related Commands**  
show running-config  
no debug all
**switchport atmf-arealink remote-area**

**Overview**  
This command enables you to configure a port or aggregator to be an AMF arealink. AMF arealinks are designed to operate between two nodes in different areas in an AMF network.

Use the `no` variant of this command to remove any AMF-arealink that may exist for the selected port or aggregated link.

This command is only available on AMF controllers and master nodes.

**Syntax**
```
switchport atmf-arealink remote-area <area-name> vlan <2-4094>
no switchport atmf-arealink
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;area-name&gt;</code></td>
<td>The name of the remote area that the port is connecting to.</td>
</tr>
<tr>
<td><code>&lt;2-4094&gt;</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Default**  
By default, no arealinks are configured

**Mode**  
Interface Configuration

**Usage**  
Run this command on the port or aggregator at both ends of the link.

Each area must have the `area-name` configured, and the same area password must exist on both ends of the link.

Running this command will automatically place the port or static aggregator into trunk mode (i.e. `switchport mode trunk`) and will synchronize the area information stored on the two nodes.

You can configure multiple arealinks between two area nodes, but only one arealink at any time will be in use. All other arealinks will block information, to prevent network storms.

**Example**  
To make a switchport 1.2.1 an arealink to the *Auckland* area on VLAN 6, use the following commands

```
controller-1# configure terminal
c controller-1(config)# interface port1.2.1
c controller-1(config-if)# switchport atmf-arealink remote-area Auckland vlan 6
```

**Related Commands**
- `atmf area`
- `atmf area password`
- `atmf virtual-link`
- `show atmf links`
AMF COMMANDS
SWITCHPORT ATMF-CROSSLINK

switchport atmf-crosslink

**Overview**
This command configures the selected port or (statically) aggregated link to be an AMF crosslink. Running this command will automatically place the port or static aggregator into trunk mode (i.e. switchport mode trunk).

The connection between two AMF masters must utilize a crosslink. Crosslinks are used to carry the AMF control information between master nodes. Multiple crosslinks can be configured between two master nodes, but only one crosslink can be active at any particular time. All other crosslinks between masters will be placed in the blocking state, in order to prevent broadcast storms.

Use the no variant of this command to remove any crosslink that may exist for the selected port or aggregated link.

**Syntax**
```
switchport atmf-crosslink
no switchport atmf-crosslink
```

**Mode**
Interface Configuration

**Usage**
Crosslinks can be used anywhere within an AMF network. They have the effect of separating the AMF network into separate domains.

Where this command is used, it is also good practice to use the `switchport trunk native vlan` command with the parameter `none` selected. This is to prevent a network storm on a topology of ring connected devices.

**Example 1**
To make a switchport 1.0.1 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-link

**Overview** This command enables you to configure a port or aggregator to be an AMF uplink/downlink. Running this command will automatically place the port or aggregator into trunk mode.

Use the no variant of this command to remove any AMF-link that may exist for the selected port or aggregated link.

**Syntax**

```
switchport atmf-link
no switchport atmf-link
```

**Mode** Interface Configuration

**Example** To make a switchport 1.0.1 an AMF crosslink, use the following commands

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# switchport atmf-link
```
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}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>join</td>
<td>AMF node join event.</td>
</tr>
<tr>
<td>leave</td>
<td>AMF node leave event.</td>
</tr>
</tbody>
</table>

**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
  !
```
Related Commands

show trigger

Node2, Node3:

trigger 5
type atmf node leave
description "E-mail on ATMF Exit"
script 1 email_me.scp
!

Related Commands
undebug atmf

**Overview**  This command is an alias for the **no** variant of the `debug atmf` command.
Introduction

Overview
This chapter provides an alphabetical reference for commands used to configure the Network Time Protocol (NTP). For more information, see the NTP Feature Overview and Configuration Guide.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Command List

• “ntp access-group” on page 2003
• “ntp authenticate” on page 2004
• “ntp authentication-key” on page 2005
• “ntp broadcastdelay” on page 2006
• “ntp master” on page 2007
• “ntp peer” on page 2008
• “ntp server” on page 2010
• “ntp source” on page 2012
• “ntp trusted-key” on page 2014
• “show counter ntp” on page 2015
• “show ntp associations” on page 2017
• “show ntp status” on page 2019
ntp access-group

**Overview**  This command creates an NTP access group, and applies a basic IP access list to it. This allows you to control access to NTP services.

The **no** variant of this command removes the configured NTP access group.

**Syntax**

```
ntp access-group [peer|query-only|serve|serve-only] [<1-99>|<1300-1999>]
```

```
no ntp access-group [peer|query-only|serve|serve-only]
```

**Parameter** | **Description**
---|---
peer | Allows time requests and NTP control queries, and allows the system to synchronize itself to a system whose address passes the access list criteria.
query-only | Allows only NTP control queries from a system whose address passes the access list criteria.
serve | Allows time requests and NTP control queries, but does not allow the system to synchronize itself to a system whose address passes the access list criteria.
serve-only | Allows only time requests from a system whose address passes the access list criteria.
<1-99> | Standard IP access list.
<1300-1999> | Expanded IP access list.

**Mode**  Global Configuration

**Examples**  To create an NTP peer access group for an extended IP access list, use the commands:

```
awplus# configure terminal
awplus(config)# ntp access-group peer 1998
```

To disable the NTP peer access group created above, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp access-group peer
```
**ntp authenticate**

**Overview**  This command enables NTP authentication. This allows NTP to authenticate the associations with other systems for security purposes.

The **no** variant of this command disables NTP authentication.

**Syntax**  
```
ntp authenticate
no ntp authenticate
```

**Mode**  Global Configuration

**Examples**

To enable NTP authentication, use the commands:

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

To disable NTP authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp authenticate
```
NTP COMMANDS
NTP AUTHENTICATION-KEY

ntp authentication-key

Overview
This command defines each of the authentication keys. Each key has a key number, a type, and a value. Currently, the only key type supported is MD5.

The no variant of this disables the authentication key assigned previously using ntp authentication-key.

Syntax
ntp authentication-key <keynumber> md5 <key>
no ntp authentication-key <keynumber> md5 <key>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;keynumber&gt;</td>
<td>&lt;1-4294967295&gt; The key number.</td>
</tr>
<tr>
<td>&lt;key&gt;</td>
<td>The authentication key.</td>
</tr>
</tbody>
</table>

Mode
Global Configuration

Examples
To define an authentication key number 134343 and a key value mystring, use the commands:

awplus# configure terminal
awplus(config)# ntp authentication-key 134343 md5 mystring

To disable the authentication key number 134343 with the key value mystring, use the commands:

awplus# configure terminal
awplus(config)# no ntp authentication-key 134343 md5 mystring
NTP BROADCASTDELAY

**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
```

**Default**
0 microsecond offset, which can only be applied with the `no` variant of this command.

**Mode**
Global Configuration

**Examples**
To set the estimated round-trip delay to 23464 microseconds for broadcast packets, use these commands:
```
awplus# configure terminal
awplus(config)# ntp broadcastdelay 23464
```
To reset the estimated round-trip delay for broadcast packets to the default setting (0 microseconds), use these commands:
```
awplus# configure terminal
awplus(config)# no ntp broadcastdelay
```
**ntp master**

**Overview**  Use this command to make the device to be an authoritative NTP server, even if the system is not synchronized to an outside time source. Note that no stratum number is set by default.

Use the **no** variant of this command to stop the device being the designated NTP server.

**Syntax**

```
ntp master [<stratum>]
no ntp master
```

**Mode**  Global Configuration

**Usage**  The stratum number is null by default and must be set using this command. The stratum levels define the distance from the reference clock and exist to prevent cycles in the hierarchy. Stratum 1 is used to indicate time servers, which are more accurate than Stratum 2 servers. For more information on the Network Time Protocol go to: [www.ntp.org](http://www.ntp.org)

**Examples**

To stop the device from being the designated NTP server use the commands:

```
awplus# configure terminal
awplus(config)# no ntp master
```

To make the device the designated NTP server with stratum number 2 use the commands:

```
awplus# configure terminal
awplus(config)# ntp master 2
```
**NTP COMMANDS**

**NTP PEER**

**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>}
```

**Mode**  Global Configuration

**Examples**  See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv4 address of 192.0.2.23:

```
awplus# configure terminal
awplus(config)# ntp peer 192.0.2.23
awplus(config)# ntp peer 192.0.2.23 prefer
awplus(config)# ntp peer 192.0.2.23 prefer version 4
awplus(config)# ntp peer 192.0.2.23 prefer version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4
awplus(config)# ntp peer 192.0.2.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of 192.0.2.23, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 192.0.2.23
```
See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv6 address of 2001:0db8:010d::1:

```
awplus# configure terminal
awplus(config)# ntp peer 2001:0db8:010d::1
awplus(config)# ntp peer 2001:0db8:010d::1 prefer
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4 key 1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4 key 1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4
awplus(config)# ntp peer 2001:0db8:010d::1 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of 2001:0db8:010d::1, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 2001:0db8:010d::1
```

**Related Commands**

ntp server

ntp source
ntp server

Overview
Use this command to configure an NTP server. This means that this system will synchronize to the other system, and not vice versa.

Use the no variant of this command to remove the configured NTP server.

Syntax
ntp server {<serveraddress>|<servername>}

ntp server {<serveraddress>|<servername>} [prefer] [key <key>] [version <version>]

no ntp server {<serveraddress>|<servername>}

Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;serveraddress&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;servername&gt;</td>
<td>Specify the server hostname. The server hostname can resolve to an IPv4 and an IPv6 address.</td>
</tr>
<tr>
<td>prefer</td>
<td>Prefer this server when possible.</td>
</tr>
<tr>
<td>key &lt;key&gt;</td>
<td>Configure the server authentication key.</td>
</tr>
<tr>
<td>version &lt;version&gt;</td>
<td>Configure for this NTP version.</td>
</tr>
</tbody>
</table>

Mode Global Configuration

Examples
See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv4 address of 192.0.1.23:

```
awplus# configure terminal
awplus(config)# ntp server 192.0.1.23
awplus(config)# ntp server 192.0.1.23 prefer
awplus(config)# ntp server 192.0.1.23 prefer version 4
awplus(config)# ntp server 192.0.1.23 prefer version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4
awplus(config)# ntp server 192.0.1.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of 192.0.1.23, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp server 192.0.1.23
```
See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv6 address of 2001:0db8:010e::2:

awplus# configure terminal
awplus(config)# ntp server 2001:0db8:010e::2
awplus(config)# ntp server 2001:0db8:010e::2 prefer
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4 key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4 key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4
awplus(config)# ntp server 2001:0db8:010e::2 key 1234

To remove an NTP peer association for this peer with an IPv6 address of 2001:0db8:010e::2, use the following commands:

awplus# configure terminal
awplus(config)# no ntp server 2001:0db8:010e::2

Related Commands
ntp peer
ntp source
**ntp source**

**Overview**
Use this command to configure an IPv4 or an IPv6 address for the NTP source interface. This command defines the socket used for NTP messages, and only applies to NTP client behavior.

Use the `no` variant of this command to remove the configured IPv4 or IPv6 address from the NTP source interface.

**Syntax**
```
ntp source <source-address>
```
```
no ntp source
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;source-address&gt;</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Default**
An IP address is selected based on the most appropriate egress interface used to reach the NTP peer if a configured NTP client source IP address is unavailable or is an invalid IP address.

**Mode**
Global Configuration

**Usage**
Adding an IPv4 or an IPv6 address allows you to select which source interface NTP uses for peering. The IPv4 or IPv6 address configured using this command is matched to the interface.

When selecting a source IP address to use for NTP messages to the peer, if the configured NTP client source IP address is unavailable then default behavior will apply, and an alternative source IP address is automatically selected. This IP address is based on the most appropriate egress interface used to reach the NTP peer. The configured NTP client source IP may be unavailable if the interface is down, or an invalid IP address is configured that does not reside on the device.

Note that this command only applies to NTP client behavior. The egress interface that the NTP messages use to reach the NTP server determined by the `ntp peer` and `ntp server` commands.

**Examples**
To configure the NTP source interface with the IPv4 address 192.0.1.23, enter the commands:
```
awplus# configure terminal
awplus(config)# ntp source 192.0.1.23
```

To configure the NTP source interface with the IPv6 address 2001:0db8:010e::2, enter the commands:
```
awplus# configure terminal
awplus(config)# ntp source 2001:0db8:010e::2
```
To remove a configured address for the NTP source interface, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp source
```

**Related Commands**
- `ntp peer`
- `ntp server`
ntp trusted-key

**Overview**
This command defines a list of trusted authentication keys. If a key is trusted, this system will be ready to synchronize to a system that uses this key in its NTP packets.

Use the **no** variant of this command to remove a configured trusted authentication key.

**Syntax**

```plaintext
ntp trusted-key <1-4294967295>
no ntp trusted-key <1-4294967295>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-4294967295&gt;</td>
<td>The specific key number.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Examples**
To define a trusted authentication key numbered 234675, use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# ntp trusted-key 234676
```

To remove the trusted authentication key numbered 234675, use the following commands:

```plaintext
awplus# configure terminal
awplus(config)# no ntp trusted-key 234676
```
show counter ntp

**Overview**  
This command displays packet counters for NTP.

**Syntax**  
`show counter ntp`

**Mode**  
User Exec and Privileged Exec

**Output**  
Figure 46-1:  Example output from the `show counter ntp` command

<table>
<thead>
<tr>
<th>NTP counters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pkts Sent</td>
<td>........ 0</td>
</tr>
<tr>
<td>Pkts Received</td>
<td>........ 70958</td>
</tr>
<tr>
<td>Pkts Processed</td>
<td>........ 0</td>
</tr>
<tr>
<td>Pkts current version</td>
<td>........ 0</td>
</tr>
<tr>
<td>Pkts old version</td>
<td>........ 0</td>
</tr>
<tr>
<td>Pkts unknown version</td>
<td>........ 0</td>
</tr>
<tr>
<td>Pkts access denied</td>
<td>........ 70958</td>
</tr>
<tr>
<td>Pkts bad length</td>
<td>........ 0</td>
</tr>
<tr>
<td>Pkts bad auth</td>
<td>........ 0</td>
</tr>
<tr>
<td>Pkts rate exceed</td>
<td>........ 0</td>
</tr>
</tbody>
</table>

Table 46-1:  Parameters in the output from the `show counter ntp` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pkts Sent</td>
<td>Total number of NTP client and server packets sent by your device.</td>
</tr>
<tr>
<td>Pkts Received</td>
<td>Total number of NTP client and server packets received by your device.</td>
</tr>
<tr>
<td>Pkts Processed</td>
<td>The number of packets processed by NTP. NTP processes a packet once it has determined that the packet is valid by checking factors such as the packet’s authentication, format, access rights and version.</td>
</tr>
<tr>
<td>Pkts current version</td>
<td>The number of version 4 NTP packets received.</td>
</tr>
<tr>
<td>Pkts old version</td>
<td>The number of NTP packets received that are from an older version, down to version 1, of NTP. NTP is compatible with these versions and processes these packets.</td>
</tr>
<tr>
<td>Pkts unknown version</td>
<td>The number of NTP packets received that are an earlier version than version 1, or a higher version than version 4. NTP cannot process these packets.</td>
</tr>
<tr>
<td>Pkts access denied</td>
<td>The number of NTP packets received that do not match any access list statements in the NTP access-groups. NTP drops these packets.</td>
</tr>
</tbody>
</table>
Table 46-1: Parameters in the output from the `show counter ntp` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pkts bad length</td>
<td>The number of NTP packets received that do not conform to the standard packet length. NTP drops these packets.</td>
</tr>
<tr>
<td>Pkts bad auth</td>
<td>The number of NTP packets received that failed authentication. NTP drops these packets. Packets can only fail authentication if NTP authentication is enabled with the <code>ntp authenticate</code> command.</td>
</tr>
<tr>
<td>Pkts rate exceed</td>
<td>The number of packets dropped because the packet rate exceeded its limits.</td>
</tr>
</tbody>
</table>

**Example**  
To display counters for NTP, use the command:

```
awplus# show counter ntp
```
show ntp associations

**Overview**  Use this command to display the status of NTP associations. Use the detail option for displaying detailed information about the associations.

**Syntax**  show ntp associations [detail]

**Mode**  User Exec and Privileged Exec

**Example**  See the sample output of the `show ntp associations` and `show ntp associations detail` commands displaying the status of NTP associations.

Table 46-2: Example output from the `show ntp associations` command

<table>
<thead>
<tr>
<th>address</th>
<th>ref clock</th>
<th>st</th>
<th>when</th>
<th>poll</th>
<th>reach</th>
<th>delay</th>
<th>offset</th>
<th>disp</th>
</tr>
</thead>
<tbody>
<tr>
<td>~192.0.2.23</td>
<td>INIT</td>
<td>16</td>
<td>-</td>
<td>512</td>
<td>000</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>
* master (synced), # master (unsynced), + selected, - candidate, ~ configured

Table 46-3: Example output from the `show ntp associations detail` command

192.0.2.23 configured, sane, valid, leap_sub, stratum 16
ref ID INIT, time 00000000.00000000 (06:28:16.000 UTC Thu Feb 7 2036)
our mode client, peer mode unspec, our poll intvl 512, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 000,
delay 0.00 msec, offset 0.0000 msec, dispersion 0.00
precision 2**-19,
org time 00000000.00000000 (06:28:16.000 UTC Thu Feb 7 2036)
xmt time cf11f2a4.cedde5e4 (00:39:00.808 UTC Tue Feb 2 2010)
filtdelay = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
fitoffset = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filterror = 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00
0 16000.00

Table 46-4: Parameters in the output from the `show ntp associations` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Peer IP address</td>
</tr>
<tr>
<td>ref clock</td>
<td>IP address for reference clock</td>
</tr>
<tr>
<td>st</td>
<td>Stratum. The number of hops between the server and the accurate time source.</td>
</tr>
<tr>
<td>poll</td>
<td>Time between NTP requests from the device to the server.</td>
</tr>
<tr>
<td>reach</td>
<td>Shows whether or not the NTP server responded to the last request.</td>
</tr>
</tbody>
</table>
NTP COMMANDS
SHOW NTP ASSOCIATIONS

Table 46-4: Parameters in the output from the `show ntp associations` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay</td>
<td>Round trip delay between the device and the server.</td>
</tr>
<tr>
<td>offset</td>
<td>Difference between the device clock and the server clock.</td>
</tr>
<tr>
<td>disp</td>
<td>Lowest measure of error associated with peer offset based on delay.</td>
</tr>
</tbody>
</table>
**show ntp status**

**Overview** Use this command to display the status of the Network Time Protocol (NTP).

**Syntax** `show ntp status`

**Mode** User Exec and Privileged Exec

**Example** See the sample output of the `show ntp status` command displaying information about the Network Time Protocol.

Figure 46-2: Example output from the `show ntp status` command

```
awplus#sh ntp status
Clock is synchronized, stratum 3, reference is 127.127.1.0
actual frequency is 0.0000 Hz, precision is 2**-19
reference time is cff1f3f2.c7c081a1 (00:44:34.780 UTC Tue Feb  2
2010)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 7947729.000 msec,
awplus#
```
Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure DHCP.

For more information, see the DHCP Feature Overview and Configuration Guide.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.
DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) COMMANDS

Command List

- “bootfile” on page 2023
- “clear ip dhcp binding” on page 2024
- “default-router” on page 2025
- “dns-server” on page 2026
- “domain-name” on page 2027
- “host” on page 2028
- “ip address dhcp” on page 2029
- “ip dhcp bootp ignore” on page 2031
- “ip dhcp leasequery enable” on page 2032
- “ip dhcp option” on page 2033
- “ip dhcp pool” on page 2035
- “ip dhcp-relay agent-option” on page 2036
- “ip dhcp-relay agent-option checking” on page 2038
- “ip dhcp-relay agent-option remote-id” on page 2039
- “ip dhcp-relay information policy” on page 2040
- “ip dhcp-relay maxhops” on page 2042
- “ip dhcp-relay max-message-length” on page 2043
- “ip dhcp-relay server-address” on page 2045
- “lease” on page 2047
- “network (DHCP)” on page 2049
- “next-server” on page 2050
- “option” on page 2051
- “probe enable” on page 2053
- “probe packets” on page 2054
- “probe timeout” on page 2055
- “probe type” on page 2056
- “range” on page 2057
- “route” on page 2058
- “service dhcp-relay” on page 2059
- “service dhcp-server” on page 2060
- “show counter dhcp-client” on page 2061
- “show counter dhcp-relay” on page 2062
- “show counter dhcp-server” on page 2065
- “show dhcp lease” on page 2067
- “show ip dhcp binding” on page 2069
• “show ip dhcp pool” on page 2071
• “show ip dhcp-relay” on page 2075
• “show ip dhcp server statistics” on page 2076
• “show ip dhcp server summary” on page 2078
• “subnet-mask” on page 2079
**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
```

**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**  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip &lt;ip-address&gt;</td>
<td>IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D.</td>
</tr>
<tr>
<td>mac &lt;mac-address&gt;</td>
<td>MAC address of the DHCP client, in hexadecimal notation in the format HHHH.HHHH.HHHH.</td>
</tr>
<tr>
<td>all</td>
<td>All DHCP bindings.</td>
</tr>
<tr>
<td>pool &lt;pool-name&gt;</td>
<td>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 &quot;quotation marks&quot;.</td>
</tr>
<tr>
<td>range &lt;low-ip-address&gt; &lt;high-ip-address&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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>]
```

**Mode**
DHCP Configuration

**Examples**
To add a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# default-router 192.168.1.2
```

To remove a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router 192.168.1.2
```

To remove all routers from the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router
```
### dns-server

**Overview**
This command adds a Domain Name System (DNS) server to the DHCP address pool you are configuring. You can use this command multiple times to create a list of DNS name servers available to the client. This sets the DNS server details using the pre-defined option 6. Note that if you add a user-defined option 6 using the `option` command, then you will override any settings created with this command.

The `no` variant of this command removes either the specified DNS server, or all DNS servers from the DHCP pool.

**Syntax**
```
dns-server <ip-address>
no dns-server [<ip-address>]
```

**Mode**
DHCP Configuration

**Examples**
To add the DNS server with the assigned IP address 192.168.1.1 to the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# dns-server 192.168.1.1
```

To remove the DNS server with the assigned IP address 192.168.1.1 from the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no dns-server 192.168.1.1
```

To remove all DNS servers from the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no dns-server
```

**Related Commands**
- `default-router`
- `option`
- `service dhcp-server`
- `show ip dhcp pool`
- `subnet-mask`
**domain-name**

**Overview**
This command adds a domain name to the DHCP address pool you are configuring. Use this command to specify the domain name that a client should use when resolving host names using the Domain Name System. This sets the domain name details using the pre-defined option 15. Note that if you add a user-defined option 15 using the `option` command, then you will override any settings created with this command.

The **no** variant of this command removes the domain name from the address pool.

**Syntax**
```
domain-name <domain-name>
```
```
no domain-name
```

**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
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;domain-name&gt;</code></td>
<td>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”.</td>
</tr>
</tbody>
</table>

**Related Commands**
- `default-router`
- `dns-server`
- `option`
- `service dhcp-server`
- `show ip dhcp pool`
- `subnet-mask`
host

**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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D</td>
</tr>
<tr>
<td><code>&lt;mac-address&gt;</code></td>
<td>MAC address of the DHCP client, in hexadecimal notation in the format HHHH.HHHH.HHHH</td>
</tr>
</tbody>
</table>

**Mode**
DHCP Configuration

**Usage**
Note that a network/mask must be configured using a `network` command before issuing a `host` command. Also note that a host address must match a network to add a static host address.

**Examples**
To add the host at 192.168.1.5 with the MAC address 000a.451d.6e34 to DHCP pool 1, use the commands:
```
awplus# configure terminal
awplus(config)# ip dhcp pool 1
awplus(dhcp-config)# network 192.168.1.0/24
awplus(dhcp-config)# host 192.168.1.5 000a.451d.6e34
```

To remove the host at 192.168.1.5 with the MAC address 000a.451d.6e34 from DHCP pool 1, use the commands:
```
awplus# configure terminal
awplus(config)# ip dhcp pool 1
awplus(dhcp-config)# no host 192.168.1.5 000a.451d.6e34
```

**Related Commands**
- `lease`
- `range`
- `show ip dhcp pool`
ip address dhcp

**Overview**  This command activates the DHCP client on the interface you are configuring. This allows the interface to use the DHCP client to obtain its IP configuration details from a DHCP server on its connected network.

The `client-id` and `hostname` parameters are identifiers that you may want to set in order to interoperate with your existing DHCP infrastructure. If neither option is needed, then the DHCP server uses the MAC address field of the request to identify the host.

The DHCP client supports the following IP configuration options:

- Option 1 - the subnet mask for your device.
- Option 3 - a list of default routers.
- Option 6 - a list of DNS servers. This list appends the DNS servers set on your device with the `ip name-server` command.
- Option 15 - a domain name used to resolve host names. This option replaces the domain name set with the `ip domain-name` command. Your device ignores this domain name if it has a domain list set using the `ip domain-list` command.
- Option 51 - lease expiration time.

The **no** variant of this command stops the interface from obtaining IP configuration details from a DHCP server.

**Syntax**  
```
ip address dhcp [client-id <interface>] [hostname <hostname>]
no ip address dhcp
```

**Parameter** | **Description**
---|---
`<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>` | 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.

**Examples**  To set the interface `vlan10` to use DHCP to obtain an IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# ip address dhcp
```
To stop the interface `vlan10` from using DHCP to obtain its IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip address dhcp
```

**Related Commands**
- `ip address`

**Validation Commands**
- `show running-config`
- `show ip interface`
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. You can then use this option when configuring a DHCP pool, by using the `option` command. Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

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**
```plaintext
ip dhcp option <1-254> [name <option-name>] [<option-type>]
no ip dhcp option [<1-254>|<option-name>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-254&gt;</code></td>
<td>The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.</td>
</tr>
<tr>
<td><code>&lt;option-name&gt;</code></td>
<td>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 &quot;quotation marks&quot;. Default: no default</td>
</tr>
<tr>
<td><code>&lt;option-type&gt;</code></td>
<td>The option value. You must specify a value that is appropriate to the option type:</td>
</tr>
</tbody>
</table>

- `ascii` An ASCII text string
- `hex` A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.
- `ip` An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually by using the option command multiple times.
- `integer` A number from 0 to 4294967295.
- `flag` A value that either sets (to 1) or unsets (to 0) a flag: `true`, `on`, or `enabled` will set the flag. `false`, `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:

```plaintext
awplus# configure terminal
awplus(config)# ip dhcp option 66 ascii
```
To define a user-defined hexadecimal string option as option 46, with the name “tcpip-node-type”, use the commands:

awplus# configure terminal
awplus(config)# ip dhcp option 46 name tcpip-node-type hex

To define a user-defined IP address option as option 175, with the name special-address, use the commands:

awplus# configure terminal
awplus(config)# ip dhcp option 175 name special-address ip

To remove the specific user-defined option with the option number 12, use the commands:

awplus# configure terminal
awplus(config)# no ip dhcp option 12

To remove the specific user-defined option with the option name perform-router-discovery, use the commands:

awplus# configure terminal
awplus(config)# no ip dhcp option perform-router-discovery

To remove all user-defined option definitions, use the commands:

awplus# configure terminal
awplus(config)# no ip dhcp option

Related Commands

default-router
dns-server
domain-name
option
service dhcp-server
show ip dhcp server summary
subnet-mask
ip dhcp pool

**Overview**  
This command will enter the configuration mode for the pool name specified. If the name specified is not associated with an existing pool, the device will create a new pool with this name, then enter the configuration mode for the new pool.

Once you have entered the DHCP configuration mode, all commands executed before the next **exit** command will apply to this pool.

You can create multiple DHCP pools on devices with multiple interfaces. This allows the device to act as a DHCP server on multiple interfaces to distribute different information to clients on the different networks.

The **no** variant of this command deletes the specific DHCP pool.

**Syntax**
```
ip dhcp pool <pool-name>
no ip dhcp pool <pool-name>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;pool-name&gt;</td>
<td>Description used to identify this DHCP pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in &quot;quotation marks&quot;.</td>
</tr>
</tbody>
</table>

**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(config-dhcp)#
```

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-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**  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 `vlan15` append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the DHCP Relay Agent from appending the DHCP Relay Agent Option 82 field on `vlan15`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# no ip dhcp-relay agent-option
```
DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) COMMANDS
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 vlan10 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```bash
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# ip dhcp-relay agent-option
awplus(config-if)# ip dhcp-relay agent-option checking
```

To stop the DHCP Relay Agent on vlan10 from checking the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```bash
awplus# configure terminal
awplus(config)# interface vlan10
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
DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) COMMANDS

IP DHCP-RELAY AGENT-OPTION REMOTE-ID

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
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>append</td>
<td>The DHCP Relay Agent appends the DHCP Relay Agent Option 82 field of the packet with its own DHCP Relay Agent Option 82 details.</td>
</tr>
<tr>
<td>drop</td>
<td>The DHCP Relay Agent discards the packet.</td>
</tr>
<tr>
<td>keep</td>
<td>The DHCP Relay Agent forwards the packet without altering the DHCP Relay Agent Option 82 field.</td>
</tr>
<tr>
<td>replace</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Mode**  Interface Configuration for a VLAN interface.
**Examples**

To make the DHCP Relay Agent listening on `vlan15` drop any client requests that already contain DHCP Relay Agent Option 82 information, use the commands:

```markdown
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# ip dhcp-relay information policy drop
```

To reset the DHCP relay information policy to the default policy for interface `vlan15`, use the commands:

```markdown
awplus# configure terminal
awplus(config)# interface vlan15
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**  

```plaintext
ip dhcp-relay maxhops <1-255>
no ip dhcp-relay maxhops
```

**Parameter**  

| <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 `vlan15`, use the commands:

```plaintext
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# ip dhcp-relay maxhops 5
```

**Related Commands**  

- `service dhcp-relay`
DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) COMMANDS

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`

**Default**
The default is 1400 bytes.

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
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 `vlan7`, use the commands:

```bash
awplus# configure terminal
awplus(config)# interface vlan7
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 **vlan7**, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan7
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv4-address&gt;</code></td>
<td>Specify the IPv4 address of the DHCP server for DHCP Relay Agent to forward client DHCP packets to, in dotted decimal notation. The IPv4 address uses the format A.B.C.D.</td>
</tr>
<tr>
<td><code>&lt;ipv6-address&gt;</code></td>
<td>Specify the IPv6 address of the DHCPv6 server for DHCPv6 Relay Agent to forward client DHCP packets to, in hexadecimal notation.</td>
</tr>
<tr>
<td><code>&lt;server-interface&gt;</code></td>
<td>Specify the interface name of the DHCPv6 server. It is only required for a DHCPv6 server with an IPv6 address.</td>
</tr>
</tbody>
</table>

**Mode**
Interface Configuration for a VLAN interface.

**Usage**
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
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 vlan10, use the commands:

awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip dhcp-relay
**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;days&gt;</td>
<td>The number of days, from 0 to 120, that the lease expiry time is configured for. Default: 1</td>
</tr>
<tr>
<td>&lt;hours&gt;</td>
<td>The number of hours, from 0 to 24, that the lease expiry time is configured for. Default: 0</td>
</tr>
<tr>
<td>&lt;minutes&gt;</td>
<td>The number of minutes, from 0 to 60, the lease expiry time is configured for. Default: 0</td>
</tr>
<tr>
<td>&lt;seconds&gt;</td>
<td>The number of seconds, from 0 to 60, the lease expiry time is configured for.</td>
</tr>
<tr>
<td>infinite</td>
<td>The lease never expires.</td>
</tr>
</tbody>
</table>

**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`
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

Mode
DHCP Configuration

Usage
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-subnet-address/prefix-length&gt;</td>
<td>The IPv4 subnet address in dotted decimal notation followed by the prefix length in slash notation.</td>
</tr>
<tr>
<td>&lt;ip-subnet-address/mask&gt;</td>
<td>The IPv4 subnet address in dotted decimal notation followed by the subnet mask in dotted decimal notation.</td>
</tr>
</tbody>
</table>
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
```

**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
```
**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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-254&gt;</td>
<td>The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.</td>
</tr>
<tr>
<td>&lt;option-name&gt;</td>
<td>Option name associated with the option.</td>
</tr>
<tr>
<td>&lt;option-value&gt;</td>
<td>The option value. You must specify a value that is appropriate to the option type:</td>
</tr>
<tr>
<td>hex</td>
<td>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.</td>
</tr>
<tr>
<td>ip</td>
<td>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.</td>
</tr>
<tr>
<td>integer</td>
<td>A number from 0 to 4294967295.</td>
</tr>
<tr>
<td>flag</td>
<td>A value of either true, on, or enabled to set the flag, or false, off or disabled to unset the flag.</td>
</tr>
</tbody>
</table>

**Mode**  
DHCP Configuration
Examples

To add the ASCII-type option named \texttt{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 \texttt{tcpip-node-type} to the pool P2 and give the option the value \texttt{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 \texttt{ip-type} option \texttt{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 \texttt{179} to a pool, and give the option the value \texttt{123456}, use the command:

```
awplus(dhcp-config)# option 179 123456
```

To add a user-defined flag option with the name \texttt{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 \texttt{tftp-server-name}, use the command:

```
awplus(dhcp-config)# no option tftp-server-name
```

Related Commands

- \texttt{dns-server}
- \texttt{ip dhcp option}
- \texttt{lease}
- \texttt{service dhcp-server}
- \texttt{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

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0-10&gt;</td>
<td>The number of probe packets sent.</td>
</tr>
</tbody>
</table>
DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) COMMANDS

PROBE TIMEOUT

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;50-5000&gt;</td>
<td>Timeout interval in milliseconds.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arp</td>
<td>Probe using ARP.</td>
</tr>
<tr>
<td>ping</td>
<td>Probe using ping.</td>
</tr>
</tbody>
</table>

**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`
**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

**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:

```bash
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:

```bash
awplus(dhcp-config)# range 192.0.2.2
```

To remove all address ranges from a pool, use the command:

```bash
awplus(dhcp-config)# no range all
```

**Related Commands**

- ip dhcp pool
- service dhcp-server
- show ip dhcp pool
route

**Overview**  This command allows the DHCP server to provide static routes to clients.

**Syntax**  
```
route A.B.C.D/M A.B.C.D {both|opt249|rfc3442}
```

**Parameter** | **Description**
--- | ---
A.B.C.D/M | Subnet for the route
A.B.C.D | Next hop for the route
both | opt249 and rfc3442
opt249 | Classless static route option for DHCP
rfc3442 | Classless static route option for DHCP

**Mode**  DHCP Configuration

**Examples**  To distribute static routes for route 0.0.0.0/0 whose next hop is 192.16.1.1 to clients using both opt249 and rfc3442, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool pubic
awplus(dhcp-config)# route 0.0.0.0/0 192.16.1.1 both
```

**Related Commands**  
- `ip dhcp pool`
service dhcp-relay

**Overview**  This command enables the DHCP Relay Agent on the device. However, on a given IP interface, no DHCP forwarding takes place until at least one DHCP server is specified to forward/relay all clients’ DHCP packets to.

The `no` variant of this command disables the DHCP Relay Agent on the device for all interfaces.

**Syntax**  
```
service dhcp-relay
no service dhcp-relay
```

**Mode**  Global Configuration

**Usage**  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`
**show counter dhcp-client**

**Overview**  This command shows counters for the DHCP client on your device.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show counter dhcp-client

**Mode**  User Exec and Privileged Exec

**Example**  To display the message counters for the DHCP client on your device, use the command:

```
awplus# show counter dhcp-client
```

**Output**  Figure 47-1: Example output from the show counter dhcp-client command

```
show counter dhcp-client
DHCPDISCOVER out ............ 10
DHCPREQUEST out ............ 34
DHCPDECLINE out ............ 4
DHCPRELEASE out ............ 0
DHCPOFFER in ............ 22
DHCPACK in ............ 18
DHCPNAK in ............ 0
```

Table 47-1: Parameters in the output of the `show counter dhcp-client` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPDISCOVER out</td>
<td>The number of DHCP Discover messages sent by the client.</td>
</tr>
<tr>
<td>DHCPREQUEST out</td>
<td>The number of DHCP Request messages sent by the client.</td>
</tr>
<tr>
<td>DHCPDECLINE out</td>
<td>The number of DHCP Decline messages sent by the client.</td>
</tr>
<tr>
<td>DHCPRELEASE out</td>
<td>The number of DHCP Release messages sent by the client.</td>
</tr>
<tr>
<td>DHCPOFFER in</td>
<td>The number of DHCP Offer messages received by the client.</td>
</tr>
<tr>
<td>DHCPACK in</td>
<td>The number of DHCP Acknowledgement messages received by the client.</td>
</tr>
<tr>
<td>DHCPNAK in</td>
<td>The number of DHCP Negative Acknowledgement messages received by the client.</td>
</tr>
</tbody>
</table>

**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 “Controlling “show” Command Output” in 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 47-2:  Example output from the show counter dhcp-relay command

```
awplus#show counter dhcp-relay

DHCP relay counters
Requests In ......... 4
Replies In ......... 4
Relayed To Server ......... 4
Relayed To Client ......... 4
Out To Server Failed ......... 0
Out To Client Failed ......... 0
Invalid hlen ......... 0
Bogus giaddr ......... 0
Corrupt Agent Option ......... 0
Missing Agent Option ......... 0
Bad Circuit ID ......... 0
Missing Circuit ID ......... 0
Bad Remote ID ......... 0
Missing Remote ID ......... 0
Option Insert Failed ......... 0
DHCPv6 Requests In ......... 0
DHCPv6 Replies In ......... 0
DHCPv6 Relayed to Server ......... 0
DHCPv6 Relayed to Client ......... 0
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests In</td>
<td>The number of DHCP Request messages received from clients.</td>
</tr>
<tr>
<td>Replies In</td>
<td>The number of DHCP Reply messages received from servers.</td>
</tr>
<tr>
<td>Relayed To Server</td>
<td>The number of DHCP Request messages relayed to servers.</td>
</tr>
<tr>
<td>Relayed To Client</td>
<td>The number of DHCP Reply messages relayed to clients.</td>
</tr>
</tbody>
</table>
**DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) COMMANDS**

**SHOW COUNTER DHCP-RELAY**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out To Server Failed</td>
<td>The number of failures when attempting to send request messages to servers. This is an internal debugging counter.</td>
</tr>
<tr>
<td>Out To Client Failed</td>
<td>The number of failures when attempting to send reply messages to clients. This is an internal debugging counter.</td>
</tr>
<tr>
<td>Invalid hlen</td>
<td>The number of incoming messages dropped due to an invalid hlen field.</td>
</tr>
<tr>
<td>Bogus giaddr</td>
<td>The number of incoming DHCP Reply messages dropped due to the bogus giaddr field.</td>
</tr>
<tr>
<td>Corrupt Agent Option</td>
<td>The number of incoming DHCP Reply messages dropped due to a corrupt relay agent information option field. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.</td>
</tr>
<tr>
<td>Missing Agent Option</td>
<td>The number of incoming DHCP Reply messages dropped due to a missing relay agent information option field. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.</td>
</tr>
<tr>
<td>Bad Circuit ID</td>
<td>The number of incoming DHCP Reply messages dropped due to a bad circuit ID. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.</td>
</tr>
<tr>
<td>Missing Circuit ID</td>
<td>The number of incoming DHCP Reply messages dropped due to a missing circuit ID. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.</td>
</tr>
</tbody>
</table>
### Dynamic Host Configuration Protocol (DHCP) Commands

**SHOW COUNTER DHCP-RELAY**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Remote ID</td>
<td>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 <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.</td>
</tr>
<tr>
<td>Missing Remote ID</td>
<td>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 <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.</td>
</tr>
<tr>
<td>Option Insert Failed</td>
<td>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 <code>ip dhcp-relay information policy</code> 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.</td>
</tr>
</tbody>
</table>

Note that the following parameters are only used on the Global VRF lite instance when DHCPv6 is running:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Requests In</td>
<td>The number of incoming DHCPv6 Request messages.</td>
</tr>
<tr>
<td>DHCPv6 Replies In</td>
<td>The number of incoming DHCPv6 Reply messages.</td>
</tr>
<tr>
<td>DHCPv6 Relayed to Server</td>
<td>The number of DHCPv6 messages relayed to the server.</td>
</tr>
<tr>
<td>DHCPv6 Relayed to Client</td>
<td>The number of DHCPv6 messages relayed to the client.</td>
</tr>
</tbody>
</table>
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 “Controlling “show” Command Output” in 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 47-3:  Example output from the show counter dhcp-server command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPDISCOVER in</td>
<td>The number of Discover messages received by the DHCP server.</td>
</tr>
<tr>
<td>DHCPREQUEST in</td>
<td>The number of Request messages received by the DHCP server.</td>
</tr>
<tr>
<td>DHCPDECLINE in</td>
<td>The number of Decline messages received by the DHCP server.</td>
</tr>
<tr>
<td>DHCPRELEASE in</td>
<td>The number of Release messages received by the DHCP server.</td>
</tr>
<tr>
<td>DHCPINFORM in</td>
<td>The number of Inform messages received by the DHCP server.</td>
</tr>
<tr>
<td>DHCPOFFER out</td>
<td>The number of Offer messages sent by the DHCP server.</td>
</tr>
<tr>
<td>DHCPACK out</td>
<td>The number of Acknowledgement messages sent by the DHCP server.</td>
</tr>
</tbody>
</table>

Table 47-2:  Parameters in the output of the **show counter dhcp-server** command
**Dynamic Host Configuration Protocol (DHCP) Commands**

**Show Counter DHCP-Server**

Related Commands

- `service dhcp-server`
- `show ip dhcp binding`
- `show ip dhcp server statistics`
- `show ip dhcp pool`

Table 47-2: Parameters in the output of the `show counter dhcp-server` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPNAK out</td>
<td>The number of Negative Acknowledgement messages sent by the DHCP server. The server sends these after receiving a request that it cannot fulfill 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.</td>
</tr>
<tr>
<td>BOOTREQUEST in</td>
<td>The number of bootp messages received by the DHCP server from bootp clients.</td>
</tr>
<tr>
<td>BOOTREPLY out</td>
<td>The number of bootp messages sent by the DHCP server to bootp clients.</td>
</tr>
</tbody>
</table>
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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>Interface name to display DHCP lease details for.</td>
</tr>
</tbody>
</table>

**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 47-4: Example output from the show dhcp lease command

<table>
<thead>
<tr>
<th>Interface vlan1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address:</td>
<td>192.168.22.4</td>
</tr>
<tr>
<td>Expires:</td>
<td>13 Mar 2007 20:10:19</td>
</tr>
<tr>
<td>Renew:</td>
<td>13 Mar 2007 18:37:06</td>
</tr>
<tr>
<td>Server:</td>
<td>Options:</td>
</tr>
<tr>
<td></td>
<td>subnet-mask</td>
</tr>
<tr>
<td></td>
<td>routers</td>
</tr>
<tr>
<td></td>
<td>dhcp-lease-time</td>
</tr>
<tr>
<td></td>
<td>dhcp-message-type</td>
</tr>
<tr>
<td></td>
<td>domain-name-servers</td>
</tr>
<tr>
<td></td>
<td>dhcp-server-identifier</td>
</tr>
<tr>
<td></td>
<td>domain-name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface vlan2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address:</td>
<td>100.8.16.4</td>
</tr>
<tr>
<td>Expires:</td>
<td>13 Mar 2007 20:15:39</td>
</tr>
<tr>
<td>Rebind:</td>
<td>13 Mar 2007 19:54:46</td>
</tr>
<tr>
<td>Server:</td>
<td>Options:</td>
</tr>
<tr>
<td></td>
<td>subnet-mask</td>
</tr>
<tr>
<td></td>
<td>routers</td>
</tr>
<tr>
<td></td>
<td>dhcp-lease-time</td>
</tr>
<tr>
<td></td>
<td>dhcp-message-type</td>
</tr>
<tr>
<td></td>
<td>dhcp-server-identifier</td>
</tr>
</tbody>
</table>

**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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  show ip dhcp binding [<ip-address>|<address-pool>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>IPv4 address of a leased IP address, in dotted decimal notation. This displays the lease information for the specified IP address.</td>
</tr>
<tr>
<td>&lt;address-pool&gt;</td>
<td>Name of an address pool. This displays the lease information for all clients within the address pool.</td>
</tr>
</tbody>
</table>

**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 47-5:  Example output from the show ip dhcp binding command

<table>
<thead>
<tr>
<th>Pool 30_2_network</th>
<th>Network 172.16.2.0/24</th>
<th>DHCP Client Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>ClientId</td>
<td>Type</td>
</tr>
<tr>
<td>172.16.2.100</td>
<td>0050.fc82.9ede</td>
<td>Dynamic</td>
</tr>
<tr>
<td>172.16.2.101</td>
<td>000e.a6ae.7c14</td>
<td>Static</td>
</tr>
<tr>
<td>172.16.2.102</td>
<td>000e.a6ae.7c4c</td>
<td>Static</td>
</tr>
<tr>
<td>172.16.2.103</td>
<td>000e.a69a.ac91</td>
<td>Static</td>
</tr>
<tr>
<td>172.16.2.104</td>
<td>00e0.189d.5e41</td>
<td>Static</td>
</tr>
<tr>
<td>172.16.2.150</td>
<td>00e0.2b04.5800</td>
<td>Static</td>
</tr>
<tr>
<td>172.16.2.167</td>
<td>4444.4400.35c3</td>
<td>Dynamic</td>
</tr>
</tbody>
</table>
Related Commands

clear ip dhcp binding
ip dhcp pool
lease
range
service dhcp-server
show ip dhcp pool
show ip dhcp pool

Overview
This command displays the configuration details and system usage of the DHCP address pools configured on the device.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Syntax
show ip dhcp pool [<address-pool>]

Mode
User Exec and Privileged Exec

Example
awplus# show ip dhcp pool

Output
Figure 47-6: Example output from the show ip dhcp pool command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;address-pool&gt;</td>
<td>Name of a specific address pool. This displays the configuration of the specified address pool only.</td>
</tr>
</tbody>
</table>

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
Dynamic Host Configuration Protocol (DHCP) Commands

Show IP DHCP Pool

**Output**

Figure 47-7: 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:
    Status: Enabled
    Type: ARP
    Packets: 2
    Timeout: 200 msecs
  Dynamic addresses:
    Total: 8
    Leased: 2
    Utilization: 25.0 %
  Static host addresses:
    Total: 1
    Leased: 1
```

Table 47-3: Parameters in the output of the `show ip dhcp pool` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool</td>
<td>Name of the pool.</td>
</tr>
<tr>
<td>network</td>
<td>Subnet and mask length of the pool.</td>
</tr>
<tr>
<td>address ranges</td>
<td>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.</td>
</tr>
<tr>
<td>static host addresses</td>
<td>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.</td>
</tr>
<tr>
<td>lease</td>
<td>The lease duration for address allocated by this pool.</td>
</tr>
</tbody>
</table>
### Table 47-3: Parameters in the output of the `show ip dhcp pool` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>domain</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>subnet mask</code></td>
<td>The subnet mask sent by the pool to clients.</td>
</tr>
<tr>
<td><code>Probe - Status</code></td>
<td>Whether lease probing is enabled or disabled.</td>
</tr>
<tr>
<td><code>Probe - Type</code></td>
<td>The lease probe type configured. Either ping or ARP.</td>
</tr>
<tr>
<td><code>Probe - Packets</code></td>
<td>The number of packets sent for each lease probe in the range 0 to 10.</td>
</tr>
<tr>
<td><code>Probe - Timeout</code></td>
<td>The timeout value in milliseconds to wait for a response after each probe packet is sent. In the range 50 to 5000.</td>
</tr>
<tr>
<td><code>dns servers</code></td>
<td>The DNS server addresses sent to by the pool to clients.</td>
</tr>
<tr>
<td><code>default-router(s)</code></td>
<td>The default router addresses sent by the pool to clients.</td>
</tr>
<tr>
<td><code>user-defined options</code></td>
<td>The list of user-defined options sent by the pool to clients.</td>
</tr>
<tr>
<td><code>Dynamic addresses - Total</code></td>
<td>The total number of IP addresses that have been configured in the pool for dynamic allocation to DHCP clients.</td>
</tr>
<tr>
<td><code>Dynamic addresses - Leased</code></td>
<td>The number of IP addresses in the pool that have been dynamically allocated (leased) to DHCP clients.</td>
</tr>
<tr>
<td><code>Dynamic addresses - Utilization</code></td>
<td>The percentage of IP addresses in the pool that are currently dynamically allocated to clients.</td>
</tr>
<tr>
<td><code>Static host addresses - Total</code></td>
<td>The number of static IP addresses configured in the pool for specific DHCP client hosts.</td>
</tr>
<tr>
<td><code>Static host addresses - Leased</code></td>
<td>The number of static IP addresses assigned to specific DHCP client hosts.</td>
</tr>
</tbody>
</table>
**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 “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
show ip dhcp-relay [interface <interface-name>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-name&gt;</td>
<td>Name of a specific interface. This displays the DHCP configuration for the specified interface only.</td>
</tr>
</tbody>
</table>

**Mode**
User Exec and Privileged Exec

**Example**
To display the DHCP Relay Agent’s configuration on the interface vlan100, use the command:

```
awplus# show ip dhcp-relay interface vlan100
```

**Output**

```
DHCP Relay Service is enabled

vlan100 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 “Controlling “show” Command Output” in 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 47-9: Example output from the `show counter dhcp server statistics` command

```
DHCP server counters
DHCPDISCOVER in .......... 20
DHCPRREQUEST in .......... 12
DHCPDECLINE in ..........  1
DHCPRELEASE in ..........  0
DHCPinFORM in ..........  0
DHCPOFFER out ..........  8
DHCPPACK out ..........  4
DHCPCNACK out ..........  0
BOOTREQUEST in ..........  0
BOOTREPLY out ..........  0
DHCPLEASEQUERY in ..........  0
DHCPLEASEUNKNOWN out ..........  0
DHCPLEASEACTIVE out ..........  0
DHCPLEASEUNASSIGNED out ..........  0
```

Table 47-4: Parameters in the output of the `show counter dhcp server statistics` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPDISCOVER in</td>
<td>The number of Discover messages received by the DHCP server.</td>
</tr>
<tr>
<td>DHCPRREQUEST in</td>
<td>The number of Request messages received by the DHCP server.</td>
</tr>
<tr>
<td>DHCPDECLINE in</td>
<td>The number of Decline messages received by the DHCP server.</td>
</tr>
</tbody>
</table>
Table 47-4: Parameters in the output of the `show counter dhcp server statistics` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPRELEASE in</td>
<td>The number of Release messages received by the DHCP server.</td>
</tr>
<tr>
<td>DHCPINFORM in</td>
<td>The number of Inform messages received by the DHCP server.</td>
</tr>
<tr>
<td>DHCPOFFER out</td>
<td>The number of Offer messages sent by the DHCP server.</td>
</tr>
<tr>
<td>DHCPACK out</td>
<td>The number of Acknowledgement messages sent by the DHCP server.</td>
</tr>
<tr>
<td>DHCPNAK out</td>
<td>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.</td>
</tr>
<tr>
<td>BOOTREQUEST in</td>
<td>The number of bootp messages received by the DHCP server from bootp clients.</td>
</tr>
<tr>
<td>BOOTREPLY out</td>
<td>The number of bootp messages sent by the DHCP server to bootp clients.umblr clients.</td>
</tr>
<tr>
<td>DHCPLEASEQUERY in</td>
<td>The number of Lease Query messages received by the DHCP server from DHCP Relay Agents.</td>
</tr>
<tr>
<td>DHCPLEASEUNKNOWN out</td>
<td>The number of Lease Unknown messages sent by the DHCP server to DHCP Relay Agents.</td>
</tr>
<tr>
<td>DHCPLEASEACTIVE out</td>
<td>The number of Lease Active messages sent by the DHCP server to DHCP Relay Agents.</td>
</tr>
<tr>
<td>DHCPLEASEUNASSIGNED out</td>
<td>The number of Lease Unassigned messages sent by the DHCP server to DHCP Relay Agents.</td>
</tr>
</tbody>
</table>

**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 “Controlling “show” Command Output” in 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 47-10: 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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mask&gt;</td>
<td>Valid IPv4 subnet mask, in dotted decimal notation.</td>
</tr>
</tbody>
</table>

**Mode**  DHCP Configuration

**Examples**  To set the subnet mask option to 255.255.255.0 for DHCP pool P2, use the commands:
```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# subnet-mask 255.255.255.0
```

To remove the subnet mask option from DHCP pool P2, use the commands:
```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no subnet-mask
```

**Related Commands**
- default-router
- dns-server
- domain-name
- next-server
- option
- service dhcp-server
- show ip dhcp pool
Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure DHCPv6. For more information, see the DHCPv6 Feature Overview and Configuration Guide.

DHCPv6 is a network protocol used to configure IPv6 hosts with IPv6 addresses and IPv6 prefixes for an IPv6 network. DHCPv6 is used instead of SLAAC (Stateless Address Autoconfiguration) at sites where centralized management of IPv6 hosts is needed. IPv6 routers require automatic configuration of IPv6 addresses and IPv6 prefixes.

DHCPv6 Prefix Delegation provides automatic configuration of IPv6 addresses and IPv6 prefixes.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

NOTE: The IPv6 addresses shown use the address space 2001:0db8::/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical networks (other than for testing purposes) nor should they appear on any public network.
DHCP FOR IPV6 (DHCPV6) COMMANDS

Command List

- “address prefix” on page 2080
- “address range” on page 2082
- “clear counter ipv6 dhcp-client” on page 2084
- “clear counter ipv6 dhcp-server” on page 2085
- “clear ipv6 dhcp binding” on page 2086
- “clear ipv6 dhcp client” on page 2088
- “dns-server (DHCPv6)” on page 2089
- “domain-name (DHCPv6)” on page 2091
- “ip dhcp-relay agent-option subscriber-id-auto-mac” on page 2092
- “ipv6 address (DHCPv6 PD)” on page 2093
- “ipv6 address dhcp” on page 2096
- “ipv6 dhcp client pd” on page 2098
- “ipv6 dhcp option” on page 2100
- “ipv6 dhcp pool” on page 2102
- “ipv6 dhcp server” on page 2104
- “ipv6 local pool” on page 2105
- “ipv6 nd prefix (DHCPv6)” on page 2107
- “link-address” on page 2109
- “option (DHCPv6)” on page 2111
- “prefix-delegation pool” on page 2113
- “show counter ipv6 dhcp-client” on page 2115
- “show counter ipv6 dhcp-server” on page 2117
- “show ipv6 dhcp” on page 2119
- “show ipv6 dhcp binding” on page 2120
- “show ipv6 dhcp interface” on page 2123
- “show ipv6 dhcp pool” on page 2125
- “sntp-address” on page 2127
**address prefix**

**Overview**
Use this command in DHCPv6 Configuration mode to specify an address prefix for address assignment with DHCPv6 server pool configuration.

Use the no variant of this command to remove the address prefix from the DHCPv6 server pool.

**Syntax**
```
address prefix <ipv6-prefix/prefix-length> [lifetime {<valid-time>|infinite} {<preferred-time>|infinite}]
no address prefix <ipv6-prefix/prefix-length>
```

**Mode**
DHCPv6 Configuration

**Default**
The default valid lifetime is 2592000 seconds and the default preferred lifetime is 604800 seconds.

**Usage**
This command creates a pool of prefixes from which addresses are assigned to clients on request, and allocates a network prefix from which the DHCPv6 Server leases addresses. This command is an alternative to using a range set using the address range command.

The DHCPv6 Server selects an IPv6 address from the range available allocated by the IPv6 prefix, randomly generating the suffix of the IPv6 address, with the specified preferred and valid lifetime leases. Leased IPv6 address are found in the...
DHCPv6 Server REPLY packet, which is located within the IANA (Identity Association for Non-temporary Addresses) IA address field in the REPLY message.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

**Examples**

To add IPv6 address prefix `2001:0db8:1::/48` for DHCPv6 server pool configuration, use the following commands:

```bash
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# address prefix 2001:0db8:1::/48
```

To remove a configured IPv6 address prefix for DHCPv6 server pool configuration, use the following commands:

```bash
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# no address prefix 2001:0db8:1::/48
```

**Related Commands**

- `address range`
- `ipv6 dhcp pool`

**Validation Commands**

- `show ipv6 dhcp binding`
- `show ipv6 dhcp pool`
address range

Overview
Use this command in DHCPv6 Configuration mode to specify an address range for address assignment with DHCPv6 server pool configuration.

Use the no variant of this command to remove an address range from the DHCPv6 server pool.

Syntax
address range <first-ipv6-address> <last-ipv6-address>[lifetime {<valid-time>|infinite} {<preferred-time>|infinite}]

no address range <first-ipv6-address> <last-ipv6-address>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;first-ipv6-address&gt;</td>
<td>Specify the first IPv6 address of the IPv6 address range, in hexadecimal notation in the format X::X::X.</td>
</tr>
<tr>
<td>&lt;last-ipv6-address&gt;</td>
<td>Specify the last IPv6 address of the IPv6 address range, in hexadecimal notation in the format X::X::X.</td>
</tr>
<tr>
<td>lifetime</td>
<td>Optional. Specify a time period for the hosts to remember router advertisements (RAs). If you specify this parameter then you must also specify a valid-time and a preferred-time value. See the Usage notes below this parameter table for a description of preferred and valid lifetimes and how these determine deprecated or invalid IPv6 addresses upon expiry.</td>
</tr>
<tr>
<td>&lt;valid-time&gt;</td>
<td>Specify a valid lifetime in seconds in the range &lt;5-31536000&gt;. The default valid lifetime is 2592000 seconds.</td>
</tr>
<tr>
<td>infinite</td>
<td>Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.</td>
</tr>
<tr>
<td>&lt;preferred-time&gt;</td>
<td>Specify a preferred lifetime in seconds in the range &lt;5-31536000&gt;. The default preferred lifetime is 604800 seconds.</td>
</tr>
</tbody>
</table>

Default
The default valid lifetime is 2592000 seconds and the default preferred lifetime is 604800 seconds.

Mode
DHCPv6 Configuration

Usage
Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.
An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

**Examples**

To add the IPv6 address range `2001:0db8:1::1` to `2001:0db8:1fff::1` for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# address range 2001:0db8:1::1 2001:0db8:1fff::1
```

To remove a configured IPv6 address range for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# no address range
```

**Related Commands**

- `address prefix`
- `ipv6 dhcp pool`

**Validation Commands**

- `show ipv6 dhcp binding`
- `show ipv6 dhcp pool`
clear counter ipv6 dhcp-client

**Overview**  Use this command in Privileged Exec mode to clear DHCPv6 client counters.

**Syntax**  clear counter ipv6 dhcp-client

**Mode**  Privileged Exec

**Example**  To clear DHCPv6 client counters, use the following command:

```
awplus# clear counter ipv6 dhcp-client
```

**Related Commands**  show counter ipv6 dhcp-client
clear counter ipv6 dhcp-server

**Overview**  Use this command in Privileged Exec mode to clear DHCPv6 server counters.

**Syntax**  clear counter ipv6 dhcp-server

**Mode**  Privileged Exec

**Example**  To clear DHCPv6 server counters, use the following command:

```
awplus# clear counter ipv6 dhcp-server
```

**Related Commands**  show counter ipv6 dhcp-server
clear ipv6 dhcp binding

**Overview**  Use this command in Privileged Exec mode to clear either a specific lease binding or the lease bindings as specified by the command parameters. The command will only take effect on dynamically allocated bindings, not statically configured bindings. This command clears binding entries on the DHCPv6 server binding table.

**Syntax**  
```
clear ipv6 dhcp binding {ipv6 <prefix>|duid <DUID>|all|pool <name>}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 &lt;prefix&gt;</td>
<td>Optional. Specify the IPv6 prefix of the DHCPv6 client, in hexadecimal notation in the format X:X::X:X.</td>
</tr>
<tr>
<td>duid &lt;DUID&gt;</td>
<td>Specify the DUID (DHCPv6 unique ID) of the DHCPv6 client.</td>
</tr>
<tr>
<td>all</td>
<td>All DHCPv6 bindings.</td>
</tr>
<tr>
<td>pool &lt;name&gt;</td>
<td>Description used to identify DHCPv6 server address pool. Valid characters are any printable character. If the name contains spaces then you must enclose these in &quot;quotation marks&quot;.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Usage**  A specific binding may be deleted by ipv6 address or duid address, or several bindings may be deleted at once using all or pool.

Note that if you specify to clear the ipv6 or duid address of what is actually a static DHCPv6 binding, an error message is displayed. If all or pool are specified and one or more static DHCPv6 bindings exist within those addresses, any dynamic entries within those addresses are cleared but any static entries are not cleared.

The clear ipv6 dhcp binding command is used as a server function. A binding table entry on the DHCPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding, all prefix lifetimes have expired, or when a user runs the clear ipv6 dhcp binding command.

If the clear ipv6 dhcp binding command is used with the optional IPv6 address parameter, only the binding for the specified client is deleted. If the clear ipv6 dhcp binding command is used without the optional IPv6 address parameter, then all automatic client bindings are deleted from the DHCPv6 bindings table.

**Example**  To clear all dynamic DHCPv6 server binding entries, use the command:
```
awplus# clear ipv6 dhcp binding all
```
DHCP FOR IPv6 (DHCPv6) COMMANDS
CLEAR IPV6 DHCP BINDING

Output  Figure 48-1:  Example output from the **clear ipv6 dhcp binding all** command

![Output Example](awplus#clear ipv6 dhcp binding all
% Deleted 1 entries)

Related Commands  **show ipv6 dhcp binding**
clear ipv6 dhcp client

**Overview**  Use this command in Privileged Exec mode to restart a DHCPv6 client on an interface.

**Syntax**  
clear ipv6 dhcp client <interface>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>Specify the interface name to restart a DHCPv6 client on.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Example**  To restart a DHCPv6 client on interface vlan1, use the following command:

awplus# clear ipv6 dhcp client vlan1

**Related Commands**  show ipv6 dhcp binding
dns-server (DHCPv6)

Overview
Use this command to add a Domain Name System (DNS) server to the DHCPv6 address pool you are configuring. You can use this command multiple times to create a list of DNS name servers available to the client. This sets the DNS server details using the pre-defined option 6. Note that if you add a user-defined option 6 using the option (DHCPv6) command, then you will override any settings created with this command.

Use the no variant of this command to remove either the specified DNS server or all DNS servers from the DHCPv6 pool.

Syntax
dns-server <ipv6-address>

no dns-server [<ipv6-address>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipv6-address&gt;</td>
<td>Specify an IPv6 address of the DNS server, in hexadecimal notation in the format X::X::X. This parameter is required when adding a DNS server to the DHCPv6 address pool. All DNS servers are removed from the DHCPv6 pool if you enter the no dns-server command without this parameter.</td>
</tr>
</tbody>
</table>

Mode
DHCPv6 Configuration

Examples
To add the DNS server with the assigned IPv6 address 2001:0db8:3000:3000::32 to the DHCPv6 server pool named P2, use the following commands:

awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# dns-server 2001:0db8:3000:3000::32

To remove the DNS server with the assigned IPv6 address 2001:0db8:3000:3000::32 from the DHCPv6 server pool named P2, use the following commands:

awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no dns-server 2001:0db8:3000:3000::32

To remove all DNS servers from the DHCPv6 server pool named P2, use the following commands:

awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no dns-server
DHCP FOR IPV6 (DHCPv6) COMMANDS

DNS-SERVER (DHCPv6)

**Related Commands**

ipv6 dhcp pool

option (DHCPv6)

show ipv6 dhcp pool
**domain-name (DHCPv6)**

**Overview**
Use this command in DHCPv6 Configuration mode to add a domain name to the DHCPv6 server address pool you are configuring.

Use the `no` variant of this command to remove a domain name from the address pool.

**Syntax**

```
domain-name <domain-name>
no domain-name
```

**Mode**
DHCPv6 Configuration

**Usage**
This command specifies the domain name that a client should use when resolving host names using the Domain Name System, and sets the domain name details using the pre-defined option 15. Note that if you add a user-defined option 15 using the `option (DHCPv6)` command, then you will override any settings created with this command.

**Examples**
To add the domain name `Engineering` to DHCPv6 server pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# domain-name Engineering
```

To remove the domain name `Engineering` from DHCPv6 server pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no domain-name Engineering
```

**Related Commands**

dns-server (DHCPv6)
option (DHCPv6)
show ipv6 dhcp pool

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;domain-name&gt;</code></td>
<td>Specify the domain name you wish to assign the DHCPv6 server address pool.</td>
</tr>
<tr>
<td></td>
<td>Valid characters are printable characters. If the name contains spaces then</td>
</tr>
</tbody>
</table>
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**

```bash
ip dhcp-relay agent-option subscriber-id-auto-mac
no ip dhcp-relay agent-option subscriber-id-auto-mac
```

**Default**

Disabled

**Usage**

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:

```bash
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.
ipv6 address (DHCPv6 PD)

**Overview**
Use this command in Interface Configuration mode for a VLAN interface to append an IPv6 address suffix to the IPv6 prefix provided by a DHCPv6 Prefix Delegation (PD) server.

Use the no variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

**Syntax**
```
ipv6 address [<ipv6-prefix-name>] <ipv6-addr/prefix-length> [eui64]
```
```
no ipv6 address [<ipv6-prefix-name>] <ipv6-addr/prefix-length> [eui64]
```

**Parameter**
- `<ipv6-prefix-name>`
  - The IPv6 prefix name advertised on the router advertisement message sent from the device. The IPv6 prefix name is delegated from the DHCPv6 Server configured for DHCPv6 Prefix-Delegation.

- `<ipv6-addr/prefix-length>`
  - Specifies the IPv6 address to be set, for example ::1/64. The IPv6 address uses the format X::X::X::X/Prefix-Length. The prefix-length is usually set between 0 and 64.

- `[eui64]`
  - EUI-64 is a method of automatically deriving the lower 64 bits of an IPv6 address, based on the switch’s MAC address.

**Mode**
- Interface Configuration for a VLAN interface.

**Mode**
- Interface Configuration for a VLAN interface or Interface Configuration for a PPP interface.

**Usage**
When specifying the eui64 parameter, the interface identifier of the IPv6 address is derived from the MAC address of the device.

For more information about EUI64, see the IPv6 Feature Overview and Configuration Guide.

**Examples**
To configure a PD prefix named prefix1 on interface vlan1 and then add an IPv6 address, use the following commands:
```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd prefix1
awplus(config-if)# ipv6 address prefix1::1/64
```
In this example, the prefix will be assigned from the pool on the PD client. The host portion or suffix will be ::1 for the last 64 bits.

To configure a PD prefix named prefix1 on interface vlan1 and then add an IPv6 address using EUI-64 identifiers, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd prefix1
awplus(config-if)# ipv6 address prefix1/64 eui64
```

In this example, the prefix will be assigned from the pool on the PD client. The host portion or suffix is created from the EUI-64 identifier of the interface for the last 64 bits.

To assign the IPv6 address 2001:0db8::a2/48 to the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address 2001:0db8::a2/48
```

To remove the IPv6 address 2001:0db8::a2/48 from the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address 2001:0db8::a2/48
```

To assign the IPv6 address to the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-fr-subif)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

To assign the eui64 derived address in the prefix 2001:db8::/64 to VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address 2001:0db8::/64 eui64
```
To remove the **eui64** derived address in the prefix 2001:db8::/32 from VLAN interface `vlan2`, use the following commands:

```bash
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address 2001:0db8::/64 eui64
```

**Validation Commands**
- `show running-config`
- `show ipv6 dhcp binding`
- `show ipv6 interface brief`
- `show ipv6 route`

**Related Commands**
- `ipv6 dhcp client pd`
- `ipv6 dhcp pool`
- `ipv6 local pool`
- `ipv6 nd prefix (DHCPv6)`
- `prefix-delegation pool`
DHCP for IPv6 (DHCPv6) Commands

IPv6 Address DHCP

ipv6 address dhcp

Overview

Use this command in Interface Configuration mode to activate the DHCPv6 client on the interface that you are configuring. This allows the interface to use the DHCPv6 client to obtain its IPv6 configuration details from a DHCPv6 server on its connected network.

Use the no variant of this command to stop the interface from obtaining IPv6 configuration details from a DHCPv6 server.

The DHCPv6 client supports the following IP configuration options:

- Option 1 - the subnet mask for your device.
- Option 3 - a list of default routers.
- Option 6 - a list of DNS servers. This list appends the DNS servers set on your device with the dns-server (DHCPv6) command.
- Option 15 - a domain name used to resolve host names. This option replaces any domain name that you have set with the domain-name (DHCPv6) command.
- Option 51 - lease expiration time.

Syntax

ipv6 address dhcp
no ipv6 address dhcp

Examples

To set the interface vlan10 to use DHCPv6 to obtain an IPv6 address, use the commands:

awplus# configure terminal
awplus(config)# interface vlan10
awplus(config)# ipv6 enable
awplus(config-if)# ipv6 address dhcp

To stop the interface vlan10 from using DHCPv6 to obtain its IPv6 address, use the commands:

awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ipv6 address dhcp

To set the PPP interface ppp0 to use DHCPv6 to obtain an IPv6 address, use the commands:

awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 address dhcp
To stop the PPP interface **ppp0** from using DHCPv6 to obtain its IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 address dhcp
```

**Related Commands**

- **ipv6 address**

**Validation Commands**

- **show running-config**
DHCP FOR IPV6 (DHCPV6) COMMANDS

IPV6 DHCP CLIENT PD

ipv6 dhcp client pd

Overview
Use this command in Interface Configuration mode to enable the DHCPv6 client process and enable requests for prefix delegation through the interface that you are configuring.

Use the no variant of this command to disable requests for prefix delegation. This is the default setting.

For further information about DHCPv6 Prefix Delegation, which is used to automate the process of assigning prefixes, see the DHCPv6 Feature Overview and Configuration Guide.

Syntax
ipv6 dhcp client pd <prefix-name>
no ipv6 dhcp client pd

Mode
Interface Configuration

Default
Prefix delegation is disabled by default on an interface.

Usage
Entering the ipv6 dhcp client pd command starts the DHCPv6 client process if not already running, and enables requests for prefix delegation through the interface on which the command is configured.

When prefix delegation is enabled and a prefix is acquired, the prefix is stored in the IPv6 prefix pool with an internal name defined by the required <prefix-name> placeholder parameter. The ipv6 address command can then refer to the prefixes stored in the IPv6 prefix pool.

Examples
To enable prefix delegation with the prefix name prefix-name on the VLAN interface vlan2, use the following commands:

awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd my-prefix-name

To disable prefix delegation on the VLAN interface vlan2, use the following commands:

awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 dhcp client pd

Parameter | Description
--- | ---
<prefix-name> | Specify an IPv6 general prefix name. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".
DHCP FOR IPV6 (DHCPv6) COMMANDS

IPV6 DHCP CLIENT PD

**Related Commands**
- clear ipv6 dhcp client
- ipv6 address (DHCPv6 PD)
- ipv6 nd prefix (DHCPv6)
- show ipv6 dhcp binding
**Overview**

Use this command in Global Configuration mode to create a user-defined DHCPv6 option. You can then use this option when configuring a DHCPv6 server address pool, by using the `option (DHCPv6)` command.

Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

Use the `no` variant of this command to remove either the specified user-defined option. This also removes user-defined options from the associated DHCPv6 server address pools.

**Syntax**

```
ipv6 dhcp option <1-254> [name <option-name>] [<option-type>]
no ipv6 dhcp option <1-254>|<option-name>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-254&gt;</code></td>
<td>The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.</td>
</tr>
<tr>
<td><code>&lt;option-name&gt;</code></td>
<td>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 &quot;quotation marks&quot;. Default: no default</td>
</tr>
<tr>
<td><code>&lt;option-type&gt;</code></td>
<td>The option value. You must specify a value that is appropriate to the option type:</td>
</tr>
<tr>
<td></td>
<td><code>ascii</code> An ASCII text string</td>
</tr>
<tr>
<td></td>
<td><code>hex</code> 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.</td>
</tr>
<tr>
<td></td>
<td><code>ipv6</code> An IPv6 address or prefix that has hexadecimal notation in the format <code>HHHH:HHHH::HHHH:HHHH</code>. To create a list of IPv6 addresses, you must add each IPv6 address individually by using the option command multiple times.</td>
</tr>
<tr>
<td></td>
<td><code>integer</code> A number from 0 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td><code>flag</code> A value that either sets (to 1) or unsets (to 0) a flag: <code>true</code>, <code>on</code>, or <code>enabled</code> will set the flag. <code>false</code>, <code>off</code> or <code>disabled</code> will unset the flag.</td>
</tr>
</tbody>
</table>

**Mode**

Global Configuration
DHCP FOR IPV6 (DHCPv6) COMMANDS

IPV6 DHCP OPTION

Examples

To define a user-defined ASCII string option as option 66, without a name, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 66 ascii
```

To define a user-defined hexadecimal string option as option 46, with the name "tcpip-node-type", use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 46 name tcpip-node-type hex
```

To define a user-defined IP address option as option 175, with the name special-address, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 175 name special-address ip
```

To remove the specific user-defined option with the option number 12, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp option 12
```

To remove the specific user-defined option with the option name perform-router-discovery, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp option perform-router-discovery
```

Related Commands

dns-server (DHCPv6)
domain-name (DHCPv6)
option (DHCPv6)
show ipv6 dhcp
ipv6 dhcp pool

**Overview**
Use this command in Global Configuration mode to enter the DHCPv6 Configuration mode for the DHCPv6 server pool name as specified in the required command parameter. If the name specified is not associated with an existing pool, the device will create a new pool with this name, then enter the configuration mode for the new pool.

Once you have entered the DHCPv6 configuration mode, all commands executed before the next `exit` command will apply to this pool.

You can create multiple DHCPv6 server pools on devices with multiple interfaces. This allows the device to act as a DHCPv6 server on multiple interfaces to distribute different information to clients on the different networks.

Use the `no` variant of this command to delete the specific DHCPv6 pool.

**Syntax**

```
ipv6 dhcp pool <DHCPv6-poolname>
no ipv6 dhcp pool <DHCPv6-poolname>
```

**Mode**
Global Configuration

**Usage**
All DHCPv6 prefix pool names must be unique. IPv6 prefix pools have a similar function to IPv4 address pools. Contrary to IPv4, a block of IPv6 addresses (an IPv6 address prefix) are assigned and not single IPv6 addresses. IPv6 prefix pools are not allowed to overlap.

Once a pool is configured, it cannot be changed. To change the configuration, you must remove then recreate a IPv6 prefix pool. All IPv6 prefixes already allocated are also freed.

**Examples**

To create the DHCPv6 pool named P2 and enter DHCPv6 configuration mode, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)#
```

To delete the DHCPv6 pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp pool P2
```
Related Commands

ipv6 local pool
option (DHCPv6)
prefix-delegation pool
show ipv6 dhcp binding
show ipv6 dhcp pool
DHCP FOR IPV6 (DHCPV6) COMMANDS

IPV6 DHCP SERVER

**ipv6 dhcp server**

- **Overview**: Use this command in Interface Configuration mode to enable DHCPv6 server for the current IPv6 configured interface to use the specified DHCPv6 server pool name.

  The DHCPv6 server service listens for DHCPv6 requests on the IPv6 configured interface. The DHCPv6 server service does not run on interfaces without IPv6 configured on them.

  Use the `no` variant of this command to disable the DHCPv6 server.

- **Syntax**: `ipv6 dhcp-server [<DHCPv6-poolname>]`
  
  `no ipv6 dhcp-server`

- **Parameter Description**:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;DHCPv6-poolname&gt;</code></td>
<td>Specify a named DHCPv6 server pool as defined with the <code>ipv6 dhcp pool</code> command. Valid characters are any printable character. If the name contains spaces then you must enclose it in &quot;quotation marks&quot;.</td>
</tr>
</tbody>
</table>

- **Mode**: Interface Configuration

- **Usage**: The `ipv6 dhcp server` command enables the DHCPv6 service on a specified interface using the pool for prefix delegation and configuration through the specified interface.

  Note that DHCPv6 client, DHCPv6 server and DHCPv6 relay are mutually exclusive on an interface. When one of the DHCPv6 functions is enabled on an interface then another DHCPv6 function cannot be enabled on the same interface.

- **Examples**: To enable the DHCPv6 server service and use the DHCPv6 pool named P2 on VLAN interface vlan2, use the following commands:

  ```
  awplus# configure terminal
  awplus(config)# interface vlan2
  awplus(config-if)# ipv6 dhcp server P2
  ```

  To disable the DHCPv6 server on VLAN interface vlan2, use the following commands:

  ```
  awplus# configure terminal
  awplus(config)# interface vlan2
  awplus(config-if)# no ipv6 dhcp server
  ```

- **Related Commands**: `ipv6 dhcp pool`, `show ipv6 dhcp binding`, `show ipv6 dhcp pool`
**Overview**  Use this command in Global Configuration mode to configure a local DHCPv6 server prefix delegation pool specifying a poolname and a prefix/prefix length. You can optionally exclude the locally assigned prefix from the pool with the `exclude-local-prefix` keyword.

Use the `no` variant of this command to remove a local DHCPv6 server prefix delegation pool specifying the poolname.

**Syntax**  
```
ipv6 local pool <DHCPv6-poolname> <delegated-prefix-name> <ipv6-prefix/prefix-length> <assigned-length> [exclude-local-prefix]
no ipv6 local pool
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;DHCPv6-poolname&gt;</code></td>
<td>Description used to identify this DHCPv6 server pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in &quot;quotation marks&quot;.</td>
</tr>
<tr>
<td><code>&lt;delegated-prefix-name&gt;</code></td>
<td>Description used to identify the delegated prefix name from the parent PD (Prefix Delegation) server. If the name contains spaces then you must enclose it in &quot;quotation marks&quot;.</td>
</tr>
<tr>
<td><code>&lt;ipv6-prefix/prefix-length&gt;</code></td>
<td>Specify an IPv6 prefix and prefix length. The prefix length indicates the length of the IPv6 prefix assigned to the pool. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.</td>
</tr>
<tr>
<td><code>&lt;assigned-length&gt;</code></td>
<td>Specify an IPv6 prefix length assigned to the user from the pool in the range &lt;1-128&gt;. Note that the value of the <code>assigned-length</code> parameter entered cannot be less than or equal to the <code>prefix-length</code> parameter value entered. An assigned length must be longer than a prefix length.</td>
</tr>
<tr>
<td><code>exclude-local-prefix</code></td>
<td>Optional. Specify this keyword to exclude the locally assigned prefix from the pool.</td>
</tr>
</tbody>
</table>

**Default**  No DHCPv6 server prefix delegation pool is configured by default.

**Mode**  Global Configuration

**Usage**  All IPv6 prefix pool names must be unique. IPv6 prefix pools have a similar function to IPv4 address pools. Contrary to IPv4, a block of IPv6 addresses (an IPv6 address prefix) are assigned and not single IPv6 addresses. IPv6 prefix pools are not allowed to overlap.
DHCP FOR IPV6 (DHCPV6) COMMANDS

IPV6 LOCAL POOL

Once a pool is configured, it cannot be changed. To change the configuration, you must remove then recreate a IPv6 prefix pool. All IPv6 prefixes already allocated are also freed.

**Examples**

To create a local DHCPv6 local pool named P2 with the IPv6 prefix and prefix length 2001:0db8::/32 with an assigned length of 64, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 local pool P2 2001:0db8::/32 64
```

To remove a configured DHCPv6 local pool, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 local pool
```

**Related Commands**

- `ipv6 dhcp pool`
- `show ipv6 dhcp pool`
DHCP FOR IPV6 (DHCPv6) COMMANDS

IPV6 ND PREFIX (DHCPv6)

**ipv6 nd prefix (DHCPv6)**

**Overview**  Use this command to specify IPv6 RA (Router Advertisement) prefix information generated from the DHCPv6 server for DHCPv6 prefix-delegation for a VLAN.

Use the **no** variant of this command to remove IPv6 RA prefix information from the DHCPv6 Server for DHCPv6 Prefix-Delegation for the interface. Use the **all** parameter with the **no** variant of this command to remove all prefix names and all prefixes for an interface.

**Syntax**

```
ipv6 nd prefix <ipv6-prefix-name>
<ipv6-prefix/length>{<valid-lifetime>|infinite}
{<preferred-lifetime>|infinite} {off-link|no-autoconfig}

no ipv6 nd prefix {<ipv6-prefix-name>|<ipv6-prefix/length>|all}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ipv6-prefix-name&gt;</code></td>
<td>The IPv6 prefix name advertised on the router advertisement message sent from the device. The IPv6 prefix name is delegated from the DHCPv6 Server configured for DHCPv6 Prefix-Delegation.</td>
</tr>
<tr>
<td><code>&lt;ipv6-prefix/length&gt;</code></td>
<td>The IPv6 prefix and prefix length advertised on the router advertisement message sent from the device. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.</td>
</tr>
<tr>
<td><code>&lt;valid-lifetime&gt;</code></td>
<td>The the period during which the specified IPv6 address prefix is valid. This can be set to a value between 5 and 315360000 seconds. Note that this period should be set to a value greater than that set for the prefix preferred-lifetime. See the Usage notes after this parameter table for a description of valid lifetime and how it determines invalid IPv6 addresses upon expiry.</td>
</tr>
<tr>
<td>infinite</td>
<td>Specifying this keyword instead of entering a value for the <code>&lt;valid-lifetime&gt;</code> parameter applies an infinite valid lifetime.</td>
</tr>
<tr>
<td><code>&lt;preferred-lifetime&gt;</code></td>
<td>Specifies the IPv6 prefix preferred lifetime. This is the period during which the IPv6 address prefix is considered current. Set this to a value between 0 and 315360000 seconds. Note that this period should be set to a value less than that set for the prefix valid-lifetime. See the Usage notes after this parameter table for a description of preferred lifetime and how it determines deprecated IPv6 addresses upon expiry.</td>
</tr>
<tr>
<td>infinite</td>
<td>Specifying this keyword instead of entering a value for the <code>&lt;preferred-lifetime&gt;</code> parameter applies an infinite valid lifetime.</td>
</tr>
<tr>
<td>off-link</td>
<td>Specify the IPv6 prefix off-link flag.</td>
</tr>
<tr>
<td>no-autoconfig</td>
<td>Specify the IPv6 prefix no autoconfiguration flag. Setting this flag indicates that the prefix is not to be used for autoconfiguration.</td>
</tr>
<tr>
<td>all</td>
<td>Specify all prefix names and all prefixes are removed when used with the no variant of this command.</td>
</tr>
</tbody>
</table>
### DHCPV6 ND PREFIX

#### Mode
- Interface Configuration for a VLAN interface.
- Interface Configuration for a VLAN interface or Interface Configuration for a PPP interface.

#### Usage
This command specifies the IPv6 prefix flags that are advertised by the router advertisement message.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

#### Examples
The following example configures the device to issue RAs (Router Advertisements) on the VLAN interface vlan4, and advertises the DHCPv6 prefix name prefix1 and the IPv6 address prefix of 2001:0db8::/32.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd prefix1
awplus(config-if)# ipv6 nd prefix prefix1 2001:0db8::/32
```

The following example resets router advertisements on the VLAN interface vlan4, so the address prefix of 2001:0db8::/32 is not advertised from the device.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/32
```

The following example removes all prefix names and prefixes from VLAN interface vlan4:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd prefix all
```

#### Related Commands
- `ipv6 address (DHCPv6 PD)`
- `ipv6 dhcp client pd`
- `ipv6 dhcp pool`
- `ipv6 local pool`
- `prefix-delegation pool`
- `show ipv6 dhcp binding`
DHCP FOR IPV6 (DHCPV6) COMMANDS

LINK-ADDRESS

link-address

Overview
Use this command in DHCPv6 Configuration mode to specify a link-address prefix within a DHCPv6 Server pool.

Note that you can only configure one link address per DHCPv6 pool. Configuring another link address in the same DHCPv6 pool overwrites the previously configured link address.

Use the no variant of this command to remove the link-address prefix from the DHCPv6 Server pool.

Syntax
link-address <ipv6-prefix/prefix-length>
no link-address

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipv6-prefix/prefix-length&gt;</td>
<td>Specify an IPv6 prefix and prefix length. The prefix length indicates the length of the IPv6 prefix assigned to the pool. The IPv6 address uses the format X::X::X::Prefix-Length. The prefix-length is usually set between 0 and 64.</td>
</tr>
</tbody>
</table>

Default
No DHCPv6 Server pool configuration link address prefix is configured by default.

Mode
DHCPv6 Configuration

Usage
Link addresses are configured in DHCPv6 Server address pools when there are remote clients that communicate via intermediate relay(s).

RELAY-FORW and RELAY-REPL relay packets contain the requesting link address source.

This command is used to match incoming requests from PD (Prefix Delegation) clients (received via an intermediate relay) to a configured delegation pool.

When an address on the incoming interface of the DHCPv6 server or a link address set in the incoming delegation request packet from the prefix delegation client matches the link-address prefix configured in the delegation pool, the DHCPv6 server is able to match and use the appropriate delegation pool for relayed delegation request messages.

If there is no match between incoming delegation request packets from the prefix delegation client and the link-address prefix configured in the delegation pool, the DHCPv6 Server does not delegate an IPv6 prefix to the requesting device.

The link address should be set to the network prefix where the prefix delegation client resides. The prefix delegation server will also need a forwarding path (IPv6 route) back to the network prefix where the prefix delegation client resides.

For more information, see the DHCPv6 Feature Overview and Configuration Guide.
**Examples**

To configure the IPv6 prefix and prefix length 2001:0db8:1::/48 as the link address for pool P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# address prefix 2001:0db8:2::/48
awplus(config-dhcp6)# link-address 2001:0db8:1::/48
```

To remove the link address, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# no link-address
```

**Related Commands**

- `ipv6 dhcp pool`
- `show ipv6 dhcp pool`
**option (DHCPv6)**

**Overview**  
Use this command in DHCPv6 Configuration mode to add a user-defined option to the DHCPv6 prefix pool you are configuring. For the **hex**, **integer**, and **flag** option types, if the option already exists, the new option overwrites the existing option’s value.

Use the **no** variant of this command to remove the specified user-defined option from the DHCPv6 server pool, or to remove all user-defined options from the DHCPv6 server pool.

**Syntax**  
```
option [<1-254>|<option-name>] <option-value>
no option [<1-254>|<option-value>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-254&gt;</td>
<td>The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.</td>
</tr>
<tr>
<td>&lt;option-name&gt;</td>
<td>Option name associated with the option.</td>
</tr>
<tr>
<td>&lt;option-value&gt;</td>
<td>The option value. You must specify a value that is appropriate to the option type:</td>
</tr>
<tr>
<td></td>
<td><strong>hex</strong> 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.</td>
</tr>
<tr>
<td></td>
<td><strong>ipv6</strong> An IPv6 prefix that has the hexadecimal X:X::X:X notation. To create a list of IPv6 prefixes, you must add each IPv6 prefix individually using this command multiple times.</td>
</tr>
<tr>
<td></td>
<td><strong>integer</strong> A number from 0 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td><strong>flag</strong> A value of either true, on, or enabled to set the flag, or false, off or disabled to unset the flag.</td>
</tr>
</tbody>
</table>

**Mode**  
DHCPv6 Configuration

**Usage**  
You must define a DHCPv6 option using the **ipv6 dhcp option** command before using the **option (DHCPv6)** command.

Note that options with an **ipv6** type can hold a list of IPv6 prefix (i.e. entries that have the X:X::X:X address format), so if the option already exists in the pool, then the new IP address is added to the list of existing IPv6 prefixes. Also note options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.
DHCP FOR IPV6 (DHCPV6) COMMANDS

Example (DHCPV6)

Examples

To add the IPv6 type option named sntp-server-addr to the pool P2 and give the option the value ipv6, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 22 name sntp_server_addr ipv6
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option sntp_server_addr ipv6
```

To add the ASCII-type option named tftp-server-name to the pool P2 and give the option the value server1, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option tftp-server-name server1
```

To add the hex-type option named tcpip-node-type to the pool P2 and give the option the value 08af, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option tcpip-node-type 08af
```

To add multiple IP addresses for the ip-type option 175, use the following commands:

```
awplus(config-dhcp6)# option 175 2001:0db8:3001::/64
awplus(config-dhcp6)# option 175 2001:0db8:3002::/64
awplus(config-dhcp6)# option 175 2001:0db8:3003::/64
```

To add the option 179 to a pool, and give the option the value 123456, use the following command:

```
awplus(config-dhcp6)# option 179 123456
```

To add a user-defined flag option with the name perform-router-discovery, use the following command:

```
awplus(config-dhcp6)# option perform-router-discovery yes
```

To clear all user-defined options from a DHCP address pool, use the following command:

```
awplus(config-dhcp6)# no option
```

To clear a user-defined option, named tftp-server-name, use the following command:

```
awplus(config-dhcp6)# no option tftp-server-name
```

Related Commands

dns-server (DHCPv6)
ipv6 dhcp option
ipv6 dhcp pool
show ipv6 dhcp pool
prefix-delegation pool

**Overview**

Use this command in DHCPv6 Configuration mode to add a DHCPv6 server prefix-delegation pool entry to the current DHCPv6 pool configuration. You must define a DHCPv6 server prefix-delegation pool using the `ipv6 dhcp pool` command before using this command.

Use the `no` variant of this command to remove a DHCPv6 server prefix-delegation pool from the current DHCPv6 pool configuration.

**Syntax**

```
prefix-delegation pool <DHCPv6-poolname> [lifetime {<valid-time>|infinite} {<preferred-time>|infinite}]
```

no prefix-delegation pool <DHCPv6-poolname>

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;DHCPv6-poolname&gt;</code></td>
<td>Description used to identify this DHCPv6 server pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in “quotation marks”.</td>
</tr>
<tr>
<td><code>lifetime</code></td>
<td>Optional. Specify a time period for the hosts to remember router advertisements (RAs). If you specify this parameter then you must also specify a <code>valid-time</code> and a <code>preferred-time</code> value. See the Usage notes below this parameter table for a description of preferred and valid lifetimes and how these determine deprecated or invalid IPv6 addresses upon expiry.</td>
</tr>
<tr>
<td><code>&lt;valid-time&gt;</code></td>
<td>Specify a valid lifetime in seconds in the range <code>&lt;5-315360000&gt;</code>.</td>
</tr>
<tr>
<td><code>infinite</code></td>
<td>Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.</td>
</tr>
<tr>
<td><code>&lt;preferred-time&gt;</code></td>
<td>Specify a valid lifetime in seconds in the range <code>&lt;5-315360000&gt;</code>.</td>
</tr>
</tbody>
</table>

**Default**

No IPv6 local prefix pool is specified by default.

**Mode**

DHCPv6 Configuration

**Usage**

The DHCPv6 server assigns prefixes dynamically from an IPv6 local prefix pool, which is configured using the `ipv6 local pool` command and is associated with a DHCPv6 configuration pool using this command. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes from the pool. After the client releases the previously assigned prefixes, the server returns the prefixes to the pool for reassignment.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source.
address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

**Example**  This example adds DHCPv6 Prefix Delegation pool pd_pool1 to DHCPv6 pool pool1:

```
awplus# configure terminal
awplus(config)# ipv6 local pool pd_pool1 2001:0db8::/48 56
awplus(config)# ipv6 dhcp pool pool1
awplus(config)# ipv6 dhcp pool pool1
awplus(config)# ipv6 local pool pd_pool1
```

**Related Commands**

ipv6 dhcp pool
ipv6 local pool
show ipv6 dhcp pool
show counter ipv6 dhcp-client

**Overview** Use this command in User Exec or Privilege Exec mode to show DHCPv6 client counter information. See `show counter ipv6 dhcp-server` for DHCPv6 server information.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show counter ipv6 dhcp-client
```

**Mode** User Exec and Privileged Exec

**Example** To display the DHCPv6 client counter information, use the command:

```
awplus# show counter ipv6 dhcp-client
```

**Output**

```
   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 48-1: Parameters in the output of the show counter ipv6 dhcp-client command**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOLICIT out</td>
<td>Displays the count of SOLICIT messages sent by the DHCPv6 client.</td>
</tr>
<tr>
<td>ADVERTISE in</td>
<td>Displays the count of ADVERTISE messages received by the DHCPv6 client.</td>
</tr>
<tr>
<td>REQUEST out</td>
<td>Displays the count of REQUEST messages sent by the DHCPv6 client.</td>
</tr>
<tr>
<td>CONFIRM out</td>
<td>Displays the count of CONFIRM messages sent by the DHCPv6 client.</td>
</tr>
<tr>
<td>RENEW out</td>
<td>Displays the count of RENEW messages sent by the DHCPv6 client.</td>
</tr>
</tbody>
</table>
### Table 48-1: Parameters in the output of the `show counter ipv6 dhcp-client` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REBIND out</td>
<td>Displays the count of REBIND messages sent by the DHCPv6 client.</td>
</tr>
<tr>
<td>REPLY in</td>
<td>Displays the count of REPLY messages received by the DHCPv6 client.</td>
</tr>
<tr>
<td>RELEASE out</td>
<td>Displays the count of RELEASE messages sent by the DHCPv6 client.</td>
</tr>
<tr>
<td>DECLINE out</td>
<td>Displays the count of DECLINE messages sent by the DHCPv6 client.</td>
</tr>
<tr>
<td>INFORMATION-REQUEST out</td>
<td>Displays the count of INFORMATION-REQUEST messages sent by the DHCPv6 client.</td>
</tr>
</tbody>
</table>
show counter ipv6 dhcp-server

**Overview**
Use this command in User Exec or Privileged Exec mode to show DHCPv6 server counter information. See `show counter ipv6 dhcp-client` for DHCPv6 client information.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**
```
show counter ipv6 dhcp-server
```

**Mode**
User Exec and Privileged Exec

**Example**
To display the DHCPv6 server counter information, use the command:
```
awplus# show counter ipv6 dhcp-server
```

**Output**
Figure 48-3: Example output from the `show counter ipv6 dhcp-server` command

```
awplus#show counter ipv6 dhcp-server
SOLICIT in ............ 20
ADVERTISE out ............ 12
REQUEST in ............ 1
CONFIRM in ............ 0
RENEW in ............ 0
REBIND in ............ 0
REPLY out ............ 0
RELEASE in ............ 0
DECLINE in ............ 0
INFORMATION-REQUEST in ............ 0
```

Table 48-2: Parameters in the output of the `show counter ipv6 dhcp-server` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOLICIT in</td>
<td>Displays the count of SOLICIT messages received by the DHCPv6 server.</td>
</tr>
<tr>
<td>ADVERTISE out</td>
<td>Displays the count of ADVERTISE messages sent by the DHCPv6 server.</td>
</tr>
<tr>
<td>REQUEST in</td>
<td>Displays the count of REQUEST messages received by the DHCPv6 server.</td>
</tr>
<tr>
<td>CONFIRM in</td>
<td>Displays the count of CONFIRM messages received by the DHCPv6 server.</td>
</tr>
<tr>
<td>RENEW in</td>
<td>Displays the count of RENEW messages received by the DHCPv6 server.</td>
</tr>
</tbody>
</table>
DHCP FOR IPV6 (DHCPv6) COMMANDS

SHOW COUNTER IPV6 DHCP-SERVER

Table 48-2: Parameters in the output of the `show counter ipv6 dhcp-server` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REBIND in</td>
<td>Displays the count of REBIND messages received by the DHCPv6 server.</td>
</tr>
<tr>
<td>REPLY out</td>
<td>Displays the count of REPLY messages sent by the DHCPv6 server.</td>
</tr>
<tr>
<td>RELEASE in</td>
<td>Displays the count of RELEASE messages received by the DHCPv6 server.</td>
</tr>
<tr>
<td>DECLINE in</td>
<td>Displays the count of DECLINE messages received by the DHCPv6 server.</td>
</tr>
<tr>
<td>INFORMATION-REQUEST in</td>
<td>Displays the count of INFORMATION-REQUEST messages received by the DHCPv6 server</td>
</tr>
</tbody>
</table>
show ipv6 dhcp

**Overview**  
Use this command in User Exec or Privileged Exec mode to show the DHCPv6 unique identifier (DUID) configured on your device.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
show ipv6 dhcp

**Mode**  
User Exec and Privileged Exec

**Usage**  
The DUID is based on the link-layer address for both DHCPv6 client and DHCPv6 server identifiers. The device uses the MAC address from the lowest interface number for the DUID.

The DUID is used by a DHCPv6 client to obtain an IPv6 address from a DHCPv6 server. A DHCPv6 server compares the DUID with its database of DUIDs and sends configuration data for an IPv6 address plus the preferred and valid lease time values to a DHCPv6 client.

**Example**  
To display the DUID configured on your device, use the command:

```
awplus# show ipv6 dhcp
```

**Output**  
Figure 48-4: Example output from the show ipv6 dhcp command

```
awplus# show ipv6 dhcp
DHCPv6 Server DUID: 0001000117ab6876001577f7ba23
```

**Related Commands**  
ipv6 address dhcp
show ipv6 dhcp binding

**Overview**  
Use this command in User Exec or Privileged Exec mode to show the IPv6 address entries that the DHCPv6 server leases to DHCPv6 clients. Note that applying this command with the optional `summary` keyword parameter displays the number of addresses per pool, but not the address or prefix entries per pool.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
`show ipv6 dhcp binding [summary]`

**Mode**  
User Exec and Privileged Exec

**Example 1**  
To display the total DHCPv6 leasing address entries for all pools, use the command:

```
awplus# show ipv6 dhcp binding summary
```

**Output**  
Figure 48-5: Example output from the `show ipv6 dhcp binding summary` command

```
awplus# show ipv6 dhcp binding summary
Pool Name               Number of Leased Addresses
-------------------------------
ia-na1                  3
ia-pd1                  5
Total in all Pools:    8
```

Table 48-3: Parameters in the output of the `show ipv6 dhcp binding summary` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool Name</td>
<td>Displays a list of all the pool names.</td>
</tr>
<tr>
<td>Number of</td>
<td>Displays the number of leased address entries for the pool.</td>
</tr>
<tr>
<td>Leased Addresses</td>
<td></td>
</tr>
<tr>
<td>Total in all Pools</td>
<td>Displays the total number of leased address entries for all pools.</td>
</tr>
</tbody>
</table>
**Example 2** To display addresses, prefixes, and lifetimes for all DHCPv6 leasing entries by pool, enter:

```
awplus# show ipv6 dhcp binding
```

**Output**

Figure 48-6: Example output from the `show ipv6 dhcp binding` command

```
awplus#show ipv6 dhcp binding
Pool ia-na1
  Address 2002:0:3c0::1
    client IAID 77f7ba23, DUID 0001000117c4bbb4001577f7ba23
    preferred lifetime 604800, valid lifetime 2592000
    starts at 20 Aug 2012 18:38:29
    expires at 19 Sep 2012 18:38:29

Pool ia-pd1
  Prefix 2002:0:3c0::/42
    client IAID 77f7ba23, DUID 0001000117c4bbb4001577f7ba23
    preferred lifetime 604800, valid lifetime 2592000
    starts at 20 Aug 2012 18:38:29
    expires at 19 Sep 2012 18:38:29
```

Table 48-4: Parameters in the output of the `show ipv6 dhcp binding` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Address delegated to the indicated IAID and DUID. See the IAID and DUID descriptions below for further information.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Prefix delegated to the indicated IAID and DUID. See the IAID and DUID descriptions below for further information.</td>
</tr>
<tr>
<td>DUID</td>
<td>DHCPv6 unique identifier (DUID) (see RFC 3315). Each DHCPv6 client has a DUID. DHCPv6 servers use DUIDs to identify clients for the association of IAs (Identity Associations) with DHCPv6 clients. DHCPv6 clients use DUIDs to identify a DHCPv6 server.</td>
</tr>
<tr>
<td>IAID</td>
<td>Identify Association Identifier (IAID) (see RFC 3315). IAIDs are identifiers for IAs (Identity Associations), where an IA is a collection of IPv6 addresses assigned to a DHCPv6 client. Each IA has an associated IAD. Each DHCPv6 client may have more than one IA assigned to it. Each IA holds one type of address.</td>
</tr>
<tr>
<td>preferred lifetime</td>
<td>The preferred lifetime setting in seconds for the specified IAID and DUID. Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires. Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.</td>
</tr>
<tr>
<td>valid lifetime</td>
<td>The valid lifetime setting in seconds for the specified IAID and DUID. An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.</td>
</tr>
</tbody>
</table>
**Table 48-4: Parameters in the output of the showipv6 dhcp binding command**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>starts at</td>
<td>The date and time at which the valid lifetime expires.</td>
</tr>
<tr>
<td>expires at</td>
<td>The date and time at which the valid lifetime expires.</td>
</tr>
</tbody>
</table>

**Related Commands**
- clear ipv6 dhcp binding
- ipv6 dhcp pool
- show ipv6 dhcp pool
**show ipv6 dhcp interface**

**Overview**  Use this command in User Exec or Privileged Exec mode to display DHCPv6 information for a specified interface, or all interfaces when entered without the interface parameter.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  
```
show ipv6 dhcp interface [interface-name]
```

**Parameter**  
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface-name&gt;</code></td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Example1**  To display DHCPv6 information for all interfaces DHCPv6 is configured on, use the command:

```
awplus# show ipv6 dhcp interface
```

**Output**  
```
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
vlan2
    is in client (Prefix-Delegation) mode
    Prefix name pd1
    prefix 2002:0:3c0::/42
    preferred lifetime 604800, valid lifetime 2592000
    starts at 20 Aug 2012 09:21:33
    expires at 19 Sep 2012 09:21:33
vlan3
    is in server mode
    Using pool : pool-1;
    Preference : 0
```
**Example 2**  To display DHCPv6 information for interface vlan2, use the command:

```
awplus# show ipv6 dhcp interface vlan2
```

**Output**  Figure 48-8:  Example output from the `show ipv6 dhcp interface vlan2` command

```
awplus# show ipv6 dhcp interface vlan2
vlan2 is in client (Prefix-Delegation) mode
  Prefix name pd1
    prefix 2002:0:3c0::/42
    preferred lifetime 604800, valid lifetime 2592000
    starts at 20 Aug 2012 09:21:33
    expires at 19 Sep 2012 09:21:33
```

Table 48-5: Parameters in the output of the `show counter dhcp-client` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface&gt;</code> is in server/client/(Prefix-Delegation) mode</td>
<td>Displays whether the specified interface is in server or client mode and whether prefix-delegation is applied to an interface.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the address of the DHCPv6 server on the interface.</td>
</tr>
<tr>
<td>Prefix name</td>
<td>Displays the IPv6 general prefix pool name, where prefixes are stored for the interface.</td>
</tr>
<tr>
<td>Using pool</td>
<td>Displays the name of the pool used by the interface.</td>
</tr>
<tr>
<td>Preference</td>
<td>Displays the preference value for the DHCPv6 server.</td>
</tr>
</tbody>
</table>

**Related Commands**  `ipv6 dhcp client pd`
show ipv6 dhcp pool

**Overview**  
Use this command in User Exec or Privileged Exec mode to display the configuration details and system usage of the DHCPv6 address pools configured on the device.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax**  

```
show ipv6 dhcp pool [DHCPv6-address-pool-name]
```

**Mode**  
User Exec and Privileged Exec

**Example**  
```
awplus# show ipv6 dhcp pool
```

**Output**  
Figure 48-9: Example output from the `show ipv6 dhcp pool` command

```
awplus# show ipv6 dhcp pool
DHCPv6 Pool: ia-na
  Address Prefix  : 1001::/64
    Lifetime: 2592000(valid), 604800(preferred)
  DNS Server: 2001::1
  DNS Server: 2001::2
  Domain Name: example.com
  Domain Name: example.co.jp
  SNTP Server: 2001::5
  SNTP Server: 2001::6
  Option Code : 150
    Value: [ASCII] test-test
DHCPv6 Pool: ia-pd
  PD Pool Name: pd1
    Prefix  : 2002::/38-42
    Lifetime: 2592000(valid), 604800(preferred)
```

Table 48-6: Parameters in the output of the `show ipv6 dhcp pool` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Pool</td>
<td>Name of the DHCPv6 pool.</td>
</tr>
<tr>
<td>Address Prefix</td>
<td>Address prefix to the DHCPv6 pool.</td>
</tr>
</tbody>
</table>
DHCP FOR IPV6 (DHCPV6) COMMANDS
SHOW IPV6 DHCP POOL

Table 48-6: Parameters in the output of the show ipv6dhcp pool command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Lifetime</td>
<td>Valid and preferred lifetimes to the DHCPv6 pool. Preferred IPv6 addresses</td>
</tr>
<tr>
<td></td>
<td>or prefixes are available to interfaces for unrestricted use and are</td>
</tr>
<tr>
<td></td>
<td>deprecated when the preferred timer expires.</td>
</tr>
<tr>
<td></td>
<td>Deprecated IPv6 addresses and prefixes are available for use and are</td>
</tr>
<tr>
<td></td>
<td>discouraged but not forbidden. A deprecated address or prefix should not</td>
</tr>
<tr>
<td></td>
<td>be used as a source address or prefix, but packets sent from deprecated</td>
</tr>
<tr>
<td></td>
<td>addresses or prefixes are delivered as expected.</td>
</tr>
<tr>
<td></td>
<td>An IPv6 address or prefix becomes invalid and is not available to an</td>
</tr>
<tr>
<td></td>
<td>interface when the valid lifetime timer expires. Invalid addresses or</td>
</tr>
<tr>
<td></td>
<td>prefixes should not appear as the source or destination for a packet.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>IPv6 address of the DNS Server</td>
</tr>
<tr>
<td>Domain name</td>
<td>URL for the domain name.</td>
</tr>
<tr>
<td>SNTP Server</td>
<td>IPv6 address of the SNTP (Simple Network Time Protocol) Server.</td>
</tr>
<tr>
<td>Option Code</td>
<td>DHCP Option code (see RFC 2132).</td>
</tr>
<tr>
<td>Option Value</td>
<td>DHCP Option value type (see RFC 2132).</td>
</tr>
</tbody>
</table>

Related Commands
ipv6 dhcp pool
**Overview**
Use this command in DHCPv6 Configuration mode to add an SNTP Server IPv6 address to a DHCPv6 Server pool.

Use the **no** variant of this command to remove an SNTP Server IPv6 address from a DHCPv6 Server pool.

**Syntax**
sntp-address <ipv6-address>
no sntp-address <ipv6-address>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipv6-address&gt;</td>
<td>Specify an SNTP Server IPv6 address, in hexadecimal notation in the format X:X::X:X.</td>
</tr>
</tbody>
</table>

**Mode**
DHCPv6 Configuration

**Examples**
The following example adds an SNTP Server IPv6 address of 2001:0db8::/32 to the DHCPv6 pool named P2:

awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# sntp-address 2001:0db8::/32

The following example removes an SNTP Server IPv6 address of 2001:0db8::/32 to the DHCPv6 pool named P2:

awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# no sntp-address 2001:0db8::/32

**Related Commands**
dns-server (DHCPv6)
domain-name (DHCPv6)
option (DHCPv6)
show ipv6 dhcp pool
Introduction

Overview  This chapter provides an alphabetical reference for commands used to configure SNMP. For more information, see:

• the SNMP MIBs Overview, for information about which MIB objects are supported.

• the SNMP Feature Overview and Configuration Guide.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.
**SNMP Commands**

**Command List**
- “debug snmp” on page 2129
- “show counter snmp-server” on page 2130
- “show debugging snmp” on page 2134
- “show running-config snmp” on page 2135
- “show snmp-server” on page 2136
- “show snmp-server community” on page 2137
- “show snmp-server group” on page 2138
- “show snmp-server user” on page 2139
- “show snmp-server view” on page 2140
- “snmp trap link-status” on page 2141
- “snmp trap link-status suppress” on page 2143
- “snmp-server” on page 2145
- “snmp-server community” on page 2147
- “snmp-server contact” on page 2148
- “snmp-server enable trap” on page 2149
- “snmp-server engineID local” on page 2152
- “snmp-server engineID local reset” on page 2154
- “snmp-server group” on page 2155
- “snmp-server host” on page 2157
- “snmp-server location” on page 2159
- “snmp-server source-interface” on page 2160
- “snmp-server startup-trap-delay” on page 2161
- “snmp-server user” on page 2162
- “snmp-server view” on page 2165
- “undebug snmp” on page 2166
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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enable or disable the display of all SNMP debugging information.</td>
</tr>
<tr>
<td>detail</td>
<td>Enable or disable the display of detailed SNMP debugging information.</td>
</tr>
<tr>
<td>error-string</td>
<td>Enable or disable the display of debugging information for SNMP error strings.</td>
</tr>
<tr>
<td>process</td>
<td>Enable or disable the display of debugging information for processed SNMP packets.</td>
</tr>
<tr>
<td>receive</td>
<td>Enable or disable the display of debugging information for received SNMP packets.</td>
</tr>
<tr>
<td>send</td>
<td>Enable or disable the display of debugging information for sent SNMP packets.</td>
</tr>
<tr>
<td>xdump</td>
<td>Enable or disable the display of hexadecimal dump debugging information for SNMP packets.</td>
</tr>
</tbody>
</table>

**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 49-1: Example output from the `show counter snmp-server` command

<table>
<thead>
<tr>
<th>SNMP-SERVER counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>inPkts</td>
</tr>
<tr>
<td>inBadVersions</td>
</tr>
<tr>
<td>inBadCommunityNames</td>
</tr>
<tr>
<td>inBadCommunityUses</td>
</tr>
<tr>
<td>inASNParseErrs</td>
</tr>
<tr>
<td>inTooBigs</td>
</tr>
<tr>
<td>inNoSuchNames</td>
</tr>
<tr>
<td>inBadValues</td>
</tr>
<tr>
<td>inReadOnlys</td>
</tr>
<tr>
<td>inGenErrs</td>
</tr>
<tr>
<td>inTotalReqVars</td>
</tr>
<tr>
<td>inTotalSetVars</td>
</tr>
<tr>
<td>inGetRequests</td>
</tr>
<tr>
<td>inGetNexts</td>
</tr>
<tr>
<td>inSetRequests</td>
</tr>
<tr>
<td>inGetResponses</td>
</tr>
<tr>
<td>inTraps</td>
</tr>
<tr>
<td>outPkts</td>
</tr>
<tr>
<td>outTooBigs</td>
</tr>
<tr>
<td>outNoSuchNames</td>
</tr>
<tr>
<td>outBadValues</td>
</tr>
<tr>
<td>outGenErrs</td>
</tr>
<tr>
<td>outGetRequests</td>
</tr>
<tr>
<td>outGetNexts</td>
</tr>
<tr>
<td>outSetRequests</td>
</tr>
<tr>
<td>outGetResponses</td>
</tr>
<tr>
<td>outTraps</td>
</tr>
<tr>
<td>UnSupportedSecLevels</td>
</tr>
<tr>
<td>NotInTimeWindows</td>
</tr>
<tr>
<td>UnknownUserNames</td>
</tr>
<tr>
<td>UnknownEngineIDs</td>
</tr>
<tr>
<td>WrongDigest</td>
</tr>
<tr>
<td>DecryptionErrors</td>
</tr>
<tr>
<td>UnknownSecModels</td>
</tr>
<tr>
<td>InvalidMsgs</td>
</tr>
<tr>
<td>UnknownPDUHandlers</td>
</tr>
</tbody>
</table>
Table 49-1: Parameters in the output of the `show counter snmp-server` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>inPkts</td>
<td>The total number of SNMP messages received by the SNMP agent.</td>
</tr>
<tr>
<td>inBadVersions</td>
<td>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.</td>
</tr>
<tr>
<td>inBadCommunityNames</td>
<td>The number of messages received by the SNMP agent with an unrecognized SNMP community name. It drops these messages.</td>
</tr>
<tr>
<td>inBadCommunityUses</td>
<td>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.</td>
</tr>
<tr>
<td>inASNParseErrs</td>
<td>The number of ASN.1 or BER errors that the SNMP agent has encountered when decoding received SNMP Messages.</td>
</tr>
<tr>
<td>inTooBigs</td>
<td>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.</td>
</tr>
<tr>
<td>inNoSuchNames</td>
<td>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.</td>
</tr>
<tr>
<td>inBadValues</td>
<td>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.</td>
</tr>
<tr>
<td>inReadOnlys</td>
<td>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.</td>
</tr>
<tr>
<td>inGenErrs</td>
<td>The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is ‘genErr’.</td>
</tr>
</tbody>
</table>
### SNMP COMMANDS

**SHOW COUNTER SNMP-SERVER**

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 49-1: Parameters in the output of the **show counter snmp-server** command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>inTotalReqVars</td>
<td>The number of MIB objects that the SNMP agent has successfully retrieved after receiving valid SNMP Get-Request and Get-Next PDUs.</td>
</tr>
<tr>
<td>inTotalSetVars</td>
<td>The number of MIB objects that the SNMP agent has successfully altered after receiving valid SNMP Set-Request PDUs.</td>
</tr>
<tr>
<td>inGetRequests</td>
<td>The number of SNMP Get-Request PDUs that the SNMP agent has accepted and processed.</td>
</tr>
<tr>
<td>inGetNexts</td>
<td>The number of SNMP Get-Next PDUs that the SNMP agent has accepted and processed.</td>
</tr>
<tr>
<td>inSetRequests</td>
<td>The number of SNMP Set-Request PDUs that the SNMP agent has accepted and processed.</td>
</tr>
<tr>
<td>inGetResponses</td>
<td>The number of SNMP Get-Response PDUs that the SNMP agent has accepted and processed.</td>
</tr>
<tr>
<td>inTraps</td>
<td>The number of SNMP Trap PDUs that the SNMP agent has accepted and processed.</td>
</tr>
<tr>
<td>outPkts</td>
<td>The number of SNMP Messages that the SNMP agent has sent.</td>
</tr>
<tr>
<td>outTooBigs</td>
<td>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.</td>
</tr>
<tr>
<td>outNoSuchNames</td>
<td>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.</td>
</tr>
<tr>
<td>outBadValues</td>
<td>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.</td>
</tr>
<tr>
<td>outGenErrs</td>
<td>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.</td>
</tr>
<tr>
<td>outGetRequests</td>
<td>The number of SNMP Get-Request PDUs that the SNMP agent has generated.</td>
</tr>
</tbody>
</table>
Table 49-1: Parameters in the output of the `show counter snmp-server` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>outGetNexts</code></td>
<td>The number of SNMP Get-Next PDUs that the SNMP agent has generated.</td>
</tr>
<tr>
<td><code>outSetRequests</code></td>
<td>The number of SNMP Set-Request PDUs that the SNMP agent has generated.</td>
</tr>
<tr>
<td><code>outGetResponses</code></td>
<td>The number of SNMP Get-Response PDUs that the SNMP agent has generated.</td>
</tr>
<tr>
<td><code>outTraps</code></td>
<td>The number of SNMP Trap PDUs that the SNMP agent has generated.</td>
</tr>
<tr>
<td><code>UnSupportedSecLevels</code></td>
<td>The number of received packets that the SNMP agent has dropped because they requested a securityLevel unknown or not available to the SNMP agent.</td>
</tr>
<tr>
<td><code>NotInTimeWindows</code></td>
<td>The number of received packets that the SNMP agent has dropped because they appeared outside of the authoritative SNMP agent's window.</td>
</tr>
<tr>
<td><code>UnknownUserNames</code></td>
<td>The number of received packets that the SNMP agent has dropped because they referenced an unknown user.</td>
</tr>
<tr>
<td><code>UnknownEngineIDs</code></td>
<td>The number of received packets that the SNMP agent has dropped because they referenced an unknown snmpEngineID.</td>
</tr>
<tr>
<td><code>WrongDigest</code></td>
<td>The number of received packets that the SNMP agent has dropped because they didn't contain the expected digest value.</td>
</tr>
<tr>
<td><code>DecryptionErrors</code></td>
<td>The number of received packets that the SNMP agent has dropped because they could not be decrypted.</td>
</tr>
<tr>
<td><code>UnknownSecModels</code></td>
<td>The number of messages received that contain a security model that is not supported by the server. Valid for SNMPv3 messages only.</td>
</tr>
<tr>
<td><code>InvalidMsgs</code></td>
<td>The number of messages received where the security model is supported but the authentication fails. Valid for SNMPv3 messages only.</td>
</tr>
<tr>
<td><code>UnknownPDUHandlers</code></td>
<td>The number of times the SNMP handler has failed to process a PDU. This is a system debugging counter.</td>
</tr>
</tbody>
</table>
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 49-2: Example output from the `show debugging snmp` command

```plaintext
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 49-3: 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:
```plaintext
awplus# show snmp-server
```

**Output**  Figure 49-4:  Example output from the `show snmp-server` command

<table>
<thead>
<tr>
<th>SNMP Server</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Protocol</td>
<td>IPv4</td>
</tr>
<tr>
<td>SNMPv3 Engine ID (configured name)</td>
<td>Not set</td>
</tr>
<tr>
<td>SNMPv3 Engine ID (actual)</td>
<td>0x80001f888021338e4747b8e607</td>
</tr>
</tbody>
</table>

**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 49-5:  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 49-6:  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 49-7: Example output from the `show snmp-server user` command

<table>
<thead>
<tr>
<th>Name</th>
<th>Group name</th>
<th>Auth</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>freddy</td>
<td>guireadgroup</td>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

**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 49-8: 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 Commands

#### 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
```

**Default**

By default, link status notifications are disabled.

**Mode**

Interface Configuration

**Usage**

The link status notifications can be enabled for the following interface types:

- switch port (e.g. port 1.0.1)
- VLAN (e.g. vlan2)
- static and dynamic link aggregation (e.g. sa2, po2)

To specify where notifications are sent, use the `snmp-server host` command. To configure the device globally to send other notifications, use the `snmp-server enable trap` command.

**Examples**

To enable SNMP to send link status notifications for ports 1.0.2 to 1.0.6, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-1.0.6
awplus(config-if)# snmp trap link-status
```

To enable SNMP to send an Allied Telesis enterprise type of link status notification for port1.0.1, use following commands:

```
awplus# configure terminal
awplus(config)# interface 1.0.1
awplus(config-if)# snmp trap link-status enterprise
```

To disable the sending of link status notifications for port 1.0.2, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no snmp trap link-status
```
**Related Commands**

- show interface
- snmp trap link-status suppress
- snmp-server enable trap
- snmp-server host
snmp trap link-status suppress

**Overview**
Use this command to enable the suppression of link status notifications (traps) for the interfaces beyond the specified threshold, in the specified interval.

Use the `no` variant of this command to disable the suppression of link status notifications for the ports.

**Syntax**
```
snmp trap link-status suppress {time {<1-60>|default}|threshold {<1-20>|default}}
```
```
no snmp trap link-status suppress
```

**Default**
By default, if link status notifications are enabled (they are enabled by default), the suppression of link status notifications is enabled: notifications that exceed the notification threshold (default 20) within the notification timer interval (default 60 seconds) are not sent.

**Mode**
Interface Configuration

**Usage**
An unstable network can generate many link status notifications. When notification suppression is enabled, a suppression timer is started when the first link status notification of a particular type (linkUp or linkDown) is sent for an interface. If the threshold number of notifications of this type is sent before the timer reaches the suppress time, any further notifications of this type generated for the interface during the interval are not sent. At the end of the interval, the sending of link status notifications resumes, until the threshold is reached in the next interval.

**Examples**
To enable the suppression of link status notifications for ports 1.0.2 to 1.0.6 after 10 notifications have been sent in 40 seconds, use following commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2-1.0.6
awplus(config-if)# snmp trap link-status suppress time 40 threshold 10
```
SNMP TRAP LINK-STATUS SUPPRESS

To disable the suppression link status notifications for port 1.0.2, use following commands:

```bash
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no snmp trap link-status suppress
```

Related Commands

- `show interface`
- `snmp trap link-status`
snmp-server

Overview
Use this command to enable the SNMP agent (server) on the device. The SNMP agent receives and processes SNMP packets sent to the device, and generates notifications (traps) that have been enabled by the snmp-server enable trap command.

Use the no variant of this command to disable the SNMP agent on the device. When SNMP is disabled, SNMP packets received by the device are discarded, and no notifications are generated. This does not remove any existing SNMP configuration.

Syntax
snmp-server [ip|ipv6]
no snmp-server [ip|ipv6]

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
SNMP COMMANDS

SNMP-SERVER

Related Commands

- show snmp-server
- show snmp-server community
- show snmp-server user
- snmp-server community
- snmp-server contact
- snmp-server enable trap
- snmp-server engineID local
- snmp-server group
- snmp-server host
- snmp-server location
- snmp-server view
snmp-server community

**Overview**  This command creates an SNMP community, optionally setting the access mode for the community. The default access mode is read only. If view is not specified, the community allows access to all the MIB objects. The SNMP communities are only valid for SNMPv1 and v2c and provide very limited security. Communities should not be used when operating SNMPv3.

The **no** variant of this command removes an SNMP community. The specified community must already exist on the device.

**Syntax**

```
snmp-server community <community-name> {view <view-name>|ro|rw|<access-list>}
no snmp-server community <community-name> [{view <view-name>|<access-list>}]  
```

**Parameter** | **Description**
---|---
<community-name> | Community name. The community name is a case sensitive string of up to 20 characters.
view | Configure SNMP view. If view is not specified, the community allows access to all the MIB objects.
$view$ | View name. The view name is a string up to 20 characters long and is case sensitive.
ro | Read-only community.
rw | Read-write community.
<access-list> | <1-99> Access list number.

**Mode**  Global Configuration

**Example**  The following command creates an SNMP community called “public” with read only access to all MIB variables from any management station.

```
awplus# configure terminal
awplus(config)# snmp-server community public ro
```

The following command removes an SNMP community called “public”

```
awplus# configure terminal
awplus(config)# no snmp-server community public
```

**Related Commands**

- show snmp-server
- show snmp-server community
- snmp-server view
snmp-server contact

**Overview**  This command sets the contact information for the system. The contact name is:
- displayed in the output of the `show system` command
- stored in the MIB object `sysContact`

The `no` variant of this command removes the contact information from the system.

**Syntax**

```
snmp-server contact <contact-info>
no snmp-server contact
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;contact-info&gt;</code></td>
<td>The contact information for the system, from 0 to 255 characters long. Valid characters are any printable character and spaces.</td>
</tr>
</tbody>
</table>

**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
awplus(config)# snmp-server contact support@alliedtelesis.co.nz
```

**Related Commands**

- `show system`
- `snmp-server location`
- `snmp-server group`
**Overview**

Use this command to enable the device to send the specified notifications (traps).

Note that the Environmental Monitoring traps are enabled by default. So you do not need to issue this command for the Environmental Monitoring traps since these are enabled by default. SNMP environmental monitoring traps defined in AT-ENVMONv2-MIB are enabled by default.

Use the `no` variant of this command to disable the sending of the specified notifications.

**Syntax**

```
snmp-server enable trap
{[atmf][atmflink][atmfnode][atmfrr][auth] [dhcpsnooping]
[epsr] [lldp] [loopprot] [mstp] [nsm] [ospf] [pim]
[power-inline] [rmon] [thrash-limit] [vcs][vrrp]}
```

```
no snmp-server enable trap
{[atmf][atmflink][atmfnode][atmfrr][auth] [dhcpsnooping]
[epsr] [lldp] [loopprot] [mstp] [nsm] [ospf] [pim]
[power-inline] [rmon] [thrash-limit] [vcs][vrrp]}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>atmf</td>
<td>AMF traps.</td>
</tr>
<tr>
<td>atmflink</td>
<td>AMF Link traps.</td>
</tr>
<tr>
<td>atmfnode</td>
<td>AMF Node traps.</td>
</tr>
<tr>
<td>atmfrr</td>
<td>AMF Reboot Rolling traps.</td>
</tr>
<tr>
<td>auth</td>
<td>Authentication failure.</td>
</tr>
<tr>
<td>dhcpsnooping</td>
<td>DHCP snooping and ARP security traps. These notifications must also be set</td>
</tr>
<tr>
<td></td>
<td>using the <code>ip dhcp snooping violation</code> command, and/or the `arp security</td>
</tr>
<tr>
<td></td>
<td>violation` command.</td>
</tr>
<tr>
<td>epsr</td>
<td>EPSR traps.</td>
</tr>
<tr>
<td>lldp</td>
<td>Link Layer Discovery Protocol (LLDP) traps. These notifications must also</td>
</tr>
<tr>
<td></td>
<td>be enabled using the <code>lldp notifications</code> command, and/or the `lldp med-</td>
</tr>
<tr>
<td></td>
<td>notifications` command.</td>
</tr>
<tr>
<td>loopprot</td>
<td>Loop Protection traps.</td>
</tr>
<tr>
<td>mstp</td>
<td>MSTP traps.</td>
</tr>
<tr>
<td>nsm</td>
<td>NSM traps.</td>
</tr>
<tr>
<td>ospf</td>
<td>OSPF traps.</td>
</tr>
<tr>
<td>pim</td>
<td>PIM traps.</td>
</tr>
<tr>
<td>power-inline</td>
<td>Power-inline traps (Power Ethernet MIB RFC 3621).</td>
</tr>
<tr>
<td>rmon</td>
<td>RMON traps.</td>
</tr>
<tr>
<td>thrash-limit</td>
<td>MAC address Thress Limiting traps.</td>
</tr>
</tbody>
</table>
SNMP COMMANDS
SNMP-SERVER ENABLE TRAP

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcs</td>
<td>VCS traps.</td>
</tr>
<tr>
<td>vrrp</td>
<td>Virtual Router Redundancy (VRRP) traps.</td>
</tr>
</tbody>
</table>

**Default**
By default, no notifications are generated.

**Mode**
Global Configuration

**Usage**
This command cannot be used to enable link status notifications globally. To enable link status notifications for particular interfaces, use the `snmp trap link-status` command.

To specify where notifications are sent, use the `snmp-server host` command.

Note that more than one trap can be configured with one command entry, and also note this command applied to notifications send by SNMP version 3.

**Examples**
To enable the device to send 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 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
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
**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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;engine-id&gt;</code></td>
<td>Specify SNMPv3 Engine ID value, a string of up to 27 characters.</td>
</tr>
<tr>
<td>default</td>
<td>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 <code>snmp-server engineID local reset</code> command to force the system to generate a new engine ID.</td>
</tr>
</tbody>
</table>

**Mode**

Global Configuration

**Usage**

All devices must have a unique engine ID which is permanently set unless it is configured by the user.

In a stacked environment, if the same engine ID was automatically generated for all members of the stack, conflicts would occur if the stack was dismantled. Therefore, each member of the stack will generate its own engine ID and the stack master's ID is used when transmitting SNMPv3 packets. Should a master failover occur, a different engine ID is transmitted. You can modify this behavior by manually assigning all stack members the same engine ID using the `snmp-server engineID local` command. However, should you decide to separate the stack and use the devices individually, you must remember to change or remove this configuration to prevent conflicts.

**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
```

**Validation Commands**  
```
show snmp-server
```

**Related Commands**  
```
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
```

**Validation Commands**

- `show snmp-server`

**Related Commands**

- `snmp-server engineID local`
**Overview**

This command is used with SNMP version 3 only, and adds an SNMP group, optionally setting the security level and view access modes for the group. The security and access views defined for the group represent the minimum required of its users in order to gain access.

The **no** variant of this command deletes an SNMP group, and is used with SNMPv3 only. The group with the specified authentication/encryption parameters must already exist.

**Syntax**

```
snmp-server group <groupname> {auth|noauth|priv} [read <readname>|write <writename>|notify <notifyname>]

no snmp-server group <groupname> {auth|noauth|priv}
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;groupname&gt;</td>
<td>Group name. The group name is a string up to 20 characters long and is case sensitive.</td>
</tr>
<tr>
<td>auth</td>
<td>Authentication.</td>
</tr>
<tr>
<td>noauth</td>
<td>No authentication and no encryption.</td>
</tr>
<tr>
<td>priv</td>
<td>Authentication and encryption.</td>
</tr>
<tr>
<td>read</td>
<td>Configure read view.</td>
</tr>
<tr>
<td>&lt;readname&gt;</td>
<td>Read view name.</td>
</tr>
<tr>
<td>write</td>
<td>Configure write view.</td>
</tr>
<tr>
<td>&lt;writename&gt;</td>
<td>Write view name. The view name is a string up to 20 characters long and is case sensitive.</td>
</tr>
<tr>
<td>notify</td>
<td>Configure notify view.</td>
</tr>
<tr>
<td>&lt;notifyname&gt;</td>
<td>Notify view name. The view name is a string up to 20 characters long and is case sensitive.</td>
</tr>
</tbody>
</table>

**Mode**

Global Configuration

**Examples**

To add SNMP group, for ordinary users, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server group usergroup noauth read useraccess write useraccess
```

To delete SNMP group **usergroup**, use the following commands

```
awplus# configure terminal
awplus(config)# no snmp-server group usergroup noauth
```
Related Commands

- `snmp-server`
- `show snmp-server`
- `show snmp-server group`
- `show snmp-server user`
SNMP COMMANDS

SNMP-SERVER HOST

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

\[
\text{snmp-server host } \{<\text{ipv4-address}>|<\text{ipv6-address}>\} \[\text{traps}\] \[\text{version 1} <\text{community-name}>\]
\]

\[
\text{snmp-server host } \{<\text{ipv4-address}>|<\text{ipv6-address}>\} \[\text{informs|traps}\] \text{version 2c } <\text{community-name}>
\]

\[
\text{snmp-server host } \{<\text{ipv4-address}>|<\text{ipv6-address}>\} \[\text{informs|traps}\] \text{version 3 } \{\text{auth|noauth|priv}\} <\text{user-name}>
\]

\[
\text{no snmp-server host } \{<\text{ipv4-address}>|<\text{ipv6-address}>\} \[\text{traps}\] \[\text{version 1} <\text{community-name}>\]
\]

\[
\text{no snmp-server host } \{<\text{ipv4-address}>|<\text{ipv6-address}>\} \[\text{informs|traps}\] \text{version 2c } <\text{community-name}>
\]

\[
\text{no snmp-server host } \{<\text{ipv4-address}>|<\text{ipv6-address}>\} \[\text{informs|traps}\] \text{version 3 } \{\text{auth|noauth|priv}\} <\text{user-name}>
\]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipv4-address&gt;</td>
<td>IPv4 trap host address in the format A.B.C.D, for example, 192.0.2.2.</td>
</tr>
<tr>
<td>&lt;ipv6-address&gt;</td>
<td>IPv6 trap host address in the format x:x:x:x for example, 2001:db8::8a2e:7334.</td>
</tr>
<tr>
<td>informs</td>
<td>Send Inform messages to this host.</td>
</tr>
<tr>
<td>traps</td>
<td>Send Trap messages to this host (default).</td>
</tr>
<tr>
<td>version</td>
<td>SNMP version to use for notification messages. Default: version 1.</td>
</tr>
<tr>
<td>1</td>
<td>Use SNMPv1 (default).</td>
</tr>
<tr>
<td>2c</td>
<td>Use SNMPv2c.</td>
</tr>
<tr>
<td>3</td>
<td>Use SNMPv3.</td>
</tr>
</tbody>
</table>
SNMP commands

SNMP-SERVER HOST

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth</td>
<td>Authentication.</td>
</tr>
<tr>
<td>noauth</td>
<td>No authentication.</td>
</tr>
<tr>
<td>priv</td>
<td>Encryption.</td>
</tr>
<tr>
<td>&lt;community-name&gt;</td>
<td>The SNMPv1 or SNMPv2c community name.</td>
</tr>
<tr>
<td>&lt;user-name&gt;</td>
<td>SNMPv3 user name.</td>
</tr>
</tbody>
</table>

**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:

```bash
awplus# configure terminal
awplus(config)# snmp-server host version 2c public 192.0.2.5
```

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:

```bash
awplus# configure terminal
awplus(config)# snmp-server host version 2c private 2001:db8::8a2e:7334
```

To remove a configured trap host of 192.0.2.5 with the SNMPv2c community name public, use the following command:

```bash
awplus# configure terminal
awplus(config)# no snmp-server host version 2c public 192.0.2.5
```

**Related Commands**

- snmp trap link-status
- snmp-server enable trap
- snmp-server view
**snmp-server location**

**Overview**  This command sets the location of the system. The location is:

- displayed in the output of the `show system` command
- stored in the MIB object `sysLocation`

The `no` variant of this command removes the configured location from the system.

**Syntax**  

```
snmp-server location <location-name>
```

```
no snmp-server location
```

**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`
**Overview**

Use this command to specify the interface that SNMP traps or informs originate from. You cannot specify an interface that does not already have an IP address assigned to the interface.

Use the `no` variant of this command to reset to the default source interface that SNMP traps or informs originate from (the Egress interface as sent from by default).

**Syntax**

```
snmp-server source-interface {traps|informs} <interface-name>
no snmp-server source-interface {traps|informs}
```

**Default**

By default the source interface is the Egress interface where traps or informs were sent from.

**Mode**

Global Configuration

**Usage**

An SNMP trap or inform sent from an SNMP server has the notification IP address of the interface where it was sent from. Use this command to monitor notifications from an interface.

**Example**

To set the interface that SNMP informs originate from to port 1.0.2 for inform packets, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server source-interface informs port1.0.2
```

To reset the interface to the default source interface (the Egress interface) that SNMP traps originate from for trap packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server source-interface traps
```

**Validation Commands**

```
show running-config
```
**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;delay-time&gt;</code></td>
<td>Specify an SNMP trap delay time in seconds in the range of 30 to 600 seconds.</td>
</tr>
</tbody>
</table>

**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 COMMANDS**

**SNMP-SERVER USER**

**Overview**  
Use this command to create or move users as members of specified groups. This command is used with SNMPv3 only.

The **no** variant of this command removes an SNMPv3 user. The specified user must already exist.

**Syntax**  
```
snmp-server user <username> <groupname> [encrypted] [auth {md5|sha} <auth-password>] [priv {des|aes} <privacy-password>]
no snmp-server user <username>
```

**Mode**  
Global Configuration

**Usage**  
Additionally this command provides the option of selecting an authentication protocol and (where appropriate) an associated password. Similarly, options are offered for selecting a privacy protocol and password.

- Note that each SNMP user must be configured on both the manager and agent entities. Where passwords are used, these passwords must be the same for both entities.
- Use the **encrypted** parameter when you want to enter already encrypted passwords in encrypted form as displayed in the running and startup configs stored on the device. For example, you may need to move a user from one

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;username&gt;</td>
<td>User name. The user name is a string up to 20 characters long and is case sensitive.</td>
</tr>
<tr>
<td>&lt;groupname&gt;</td>
<td>Group name. The group name is a string up to 20 characters long and is case sensitive.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Use the encrypted parameter when you want to enter encrypted passwords.</td>
</tr>
<tr>
<td>auth</td>
<td>Authentication protocol.</td>
</tr>
<tr>
<td>md5</td>
<td>MD5 Message Digest Algorithms.</td>
</tr>
<tr>
<td>sha</td>
<td>SHA Secure Hash Algorithm.</td>
</tr>
<tr>
<td>&lt;auth-password&gt;</td>
<td>Authentication password. The password is a string of 8 to 20 characters long and is case sensitive.</td>
</tr>
<tr>
<td>priv</td>
<td>Privacy protocol.</td>
</tr>
<tr>
<td>des</td>
<td>DES Data Encryption Standard.</td>
</tr>
<tr>
<td>aes</td>
<td>AES Advanced Encryption Standards.</td>
</tr>
<tr>
<td>&lt;privacy-password&gt;</td>
<td>Privacy password. The password is a string of 8 to 20 characters long and is case sensitive.</td>
</tr>
</tbody>
</table>
group to another group and keep the same passwords for the user instead of removing the user to apply new passwords.

- User passwords are entered using plaintext without the `encrypted` parameter and are encrypted according to the authentication and privacy protocols selected.
- User passwords are viewed as encrypted passwords in running and startup configs shown from `show running-config` and `show startup-config` commands respectively. Copy and paste encrypted passwords from running-configs or startup-configs to avoid entry errors.

**Examples**

To add SNMP user `authuser` as a member of group `usergroup`, with authentication protocol `md5`, authentication password `Authpass`, privacy protocol `des` and privacy password `Privpass`, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server user authuser usergroup auth md5 Authpass priv des Privpass
```

Validate the user is assigned to the group using the `show snmp-server user` command:

```
awplus#show snmp-server user
Name          Group name         Auth   Privacy
------------  --------------  ------  --------
authuser      usergroup        md5    des
```

To enter existing SNMP user `authuser` with existing passwords as a member of group `newusergroup` with authentication protocol `md5` plus the encrypted authentication password `0x1c74b9c22118291b0ce0cd883f8dab6b74`, privacy protocol `des` plus the encrypted privacy password `0x0e0133db5453ebd03822b004eeacb6608f`, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server user authuser newusergroup encrypted auth md5 0x1c74b9c22118291b0ce0cd883f8dab6b74 priv des 0xe0133db5453ebd03822b004eeacb6608f
```

**NOTE:** Copy and paste the encrypted passwords from the `running-config` or the `startup-config` displayed, using the `show running-config` and `show startup-config` commands respectively, into the command line to avoid key stroke errors issuing this command.

Validate the user has been moved from the first group using the `show snmp-server user` command:

```
awplus#show snmp-server user
Name          Group name         Auth   Privacy
------------  --------------  ------  --------
authuser      newusergroup      md5    des
```
To delete SNMP user authuser, use the following commands:

awplus# configure terminal
awplus(config)# no snmp-server user authuser

Related Commands

- show snmp-server user
- snmp-server view
snmp-server view

**Overview**
Use this command to create an SNMP view that specifies a sub-tree of the MIB. Further sub-trees can then be added by specifying a new OID to an existing view. Views can be used in SNMP communities or groups to control the remote manager’s access.

*NOTE:* The object identifier must be specified in a sequence of integers separated by decimal points.

The **no** variant of this command removes the specified view on the device. The view must already exist.

**Syntax**

```
snmp-server view <view-name> <mib-name> {included|excluded}
no snmp-server view <view-name>
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;view-name&gt;</code></td>
<td>SNMP server view name. The view name is a string up to 20 characters long and is case sensitive.</td>
</tr>
<tr>
<td><code>&lt;mib-name&gt;</code></td>
<td>Object identifier of the MIB.</td>
</tr>
<tr>
<td>included</td>
<td>Include this OID in the view.</td>
</tr>
<tr>
<td>excluded</td>
<td>Exclude this OID in the view.</td>
</tr>
</tbody>
</table>

**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
**Overview**  This command applies the functionality of the no `debug snmp` command.
Introduction

Overview

LLDP and LLDP-MED can be configured using the commands in this chapter, or by using SNMP with the LLDP-MIB and LLDP-EXT-DOT1-MIB (see the SNMP MIBs Overview).

The Voice VLAN feature can be configured using commands in the VLAN Commands chapter.

For more information about LLDP, see the LLDP Feature Overview and Configuration Guide.

LLDP can transmit a lot of data about the network. Typically, the network information gathered using LLDP is transferred to a Network Management System by SNMP. For security reasons, we recommend using SNMPv3 for this purpose (see the SNMP Feature Overview and Configuration Guide).

LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static or dynamic channel groups, but not on the channel groups themselves.
LLDP COMMANDS

**Command List**

- “clear lldp statistics” on page 2168
- “clear lldp table” on page 2169
- “debug lldp” on page 2170
- “lldp faststart-count” on page 2172
- “lldp holdtime-multiplier” on page 2173
- “lldp management-address” on page 2174
- “lldp med-notifications” on page 2175
- “lldp med-tlv-select” on page 2176
- “lldp non-strict-med-tlv-order-check” on page 2178
- “lldp notification-interval” on page 2179
- “lldp notifications” on page 2180
- “lldp port-number-type” on page 2181
- “lldp reinit” on page 2182
- “lldp run” on page 2183
- “lldp timer” on page 2184
- “lldp tlv-select” on page 2185
- “lldp transmit receive” on page 2187
- “lldp tx-delay” on page 2188
- “location civic-location configuration” on page 2189
- “location civic-location identifier” on page 2194
- “location civic-location-id” on page 2195
- “location coord-location configuration” on page 2196
- “location coord-location identifier” on page 2198
- “location coord-location-id” on page 2199
- “location elin-location” on page 2200
- “location elin-location-id” on page 2201
- “show debugging lldp” on page 2202
- “show lldp” on page 2204
- “show lldp interface” on page 2206
- “show lldp local-info” on page 2208
- “show lldp neighbors” on page 2213
- “show lldp neighbors detail” on page 2215
- “show lldp statistics” on page 2219
- “show lldp statistics interface” on page 2221
- “show location” on page 2223
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>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports for which the statistics are to be cleared.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec

**Examples**  
To clear the LLDP statistics on ports 1.0.1 and 1.0.6, use the command:

awplus# clear lldp statistics interface port1.0.1, port1.0.6

To clear all LLDP statistics for all ports, use the command:

awplus# clear lldp statistics

**Related Commands**  
show lldp statistics  
show lldp statistics interface
**clear lldp table**

**Overview**  
This command clears the table of LLDP information received from neighbors through specified ports. If no port list is supplied, neighbor information is cleared for all ports.

**Syntax**  
clear lldp table [interface <port-list>]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports for which the neighbor information table is to be cleared.</td>
</tr>
</tbody>
</table>

**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
```  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rx</td>
<td>LLDP receive debug.</td>
</tr>
<tr>
<td>rxpkt</td>
<td>Raw LLDPDUs received in hex format.</td>
</tr>
<tr>
<td>tx</td>
<td>LLDP transmit debug.</td>
</tr>
<tr>
<td>txpkt</td>
<td>Raw Tx LLDPDUs transmitted in hex format.</td>
</tr>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports for which debug is to be configured.</td>
</tr>
<tr>
<td>operation</td>
<td>Debug for LLDP internal operation on the switch.</td>
</tr>
<tr>
<td>all</td>
<td>Disables all LLDP debugging for all ports.</td>
</tr>
</tbody>
</table>

**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
```

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-10&gt;</td>
<td>The number of fast start advertisements to send.</td>
</tr>
</tbody>
</table>
**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
```

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipaddr&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Default**
The local loopback interface primary IPv4 address if set, else the primary IPv4 interface address of the lowest numbered VLAN the port belongs to, else the MAC address of the device’s baseboard if no VLAN IP addresses are configured for the port.

**Mode**
Interface Configuration

**Usage**
To see the management address that will be advertised, use the **show lldp interface** command or **show lldp local-info** command.

**Examples**
To set the management address advertised by ports 1.0.1 and 1.0.6, to be 192.168.1.6, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp management-address 192.168.1.6
```

To clear the user-configured management address advertised by ports 1.0.1 and 1.0.6, and revert to using the default address, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp management-address
```

**Related Commands**
- show lldp interface
- show lldp local-info
lldp med-notifications

**Overview**
Use this command to enable LLDP to send LLDP-MED Topology Change Detected SNMP notifications relating to the specified ports. The switch sends an SNMP event notification when a new LLDP-MED compliant IP Telephony device is connected to or disconnected from a port on the switch.

Use the `no` variant of this command to disable the sending of LLDP-MED Topology Change Detected notifications relating to the specified ports.

**Syntax**
```
lldp med-notifications
no lldp med-notifications
```

**Default**
The sending of LLDP-MED notifications is disabled by default.

**Mode**
Interface Configuration

**Examples**
To enable the sending of LLDP-MED Topology Change Detected notifications relating to ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp med-notifications
```
To disable the sending of LLDP-MED notifications relating to ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-notifications
```

**Related Commands**
- `lldp notification-interval`
- `lldp notifications`
- `snmp-server enable trap`
- `show lldp interface`
**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] 
} 
```

```
no lldp med-tlv-select {
    [capabilities] [network-policy] 
    [location] [power-management-ext] [inventory-management] 
} 
```

```
no lldp med-tlv-select all 
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>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 <code>lldp tlv-select</code> command.</td>
</tr>
<tr>
<td>network-policy</td>
<td>Network Policy TLV. This TLV is transmitted if Voice VLAN parameters have been configured using the commands:</td>
</tr>
<tr>
<td>location</td>
<td>Location Identification TLV. This TLV is transmitted if location information has been configured using the commands:</td>
</tr>
<tr>
<td>power-management-ext</td>
<td>Extended Power-via-MDI TLV. This TLV is transmitted if the port is PoE capable, and PoE is enabled (power-inline enable command).</td>
</tr>
<tr>
<td>inventory-management</td>
<td>Inventory Management TLV Set, including the following TLVs:</td>
</tr>
<tr>
<td></td>
<td>• Hardware Revision</td>
</tr>
<tr>
<td></td>
<td>• Firmware Revision</td>
</tr>
<tr>
<td></td>
<td>• Software Revision</td>
</tr>
<tr>
<td></td>
<td>• Serial Number</td>
</tr>
<tr>
<td></td>
<td>• Manufacturer Name</td>
</tr>
<tr>
<td></td>
<td>• Model Name</td>
</tr>
<tr>
<td></td>
<td>• Asset ID</td>
</tr>
<tr>
<td>all</td>
<td>All LLDP-MED Organizationally Specific TLVs.</td>
</tr>
</tbody>
</table>
LLDP COMMANDS
LLDP MED-TLV-SELECT

**Default**
By default LLDP-MED Capabilities, Network Policy, Location Identification and Extended Power-via-MDI TLVs are enabled. Therefore, if LLDP is enabled using the `lldp run` command, by default LLDP-MED advertisements are transmitted on ports that detect LLDP-MED neighbors connected to them.

**Mode**
Interface Configuration

**Usage**
LLDP-MED TLVs are only sent in advertisements via a port if there is an LLDP-MED-capable device connected to it. To see whether there are LLDP-MED capable devices connected to the ports, use the `show lldp neighbors` command.

**Examples**
To enable inclusion of the Inventory TLV Set in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp med-tlv-select inventory-management
```

To exclude the Inventory TLV Set in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-tlv-select inventory-management
```

To disable LLDP-MED advertisements transmitted via ports 1.0.1 and 1.0.6, disable all these TLVs using the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-tlv-select all
```

**Related Commands**
- `lldp tlv-select`
- `location elin-location-id`
- `location civic-location identifier`
- `location civic-location configuration`
- `location coord-location identifier`
- `location coord-location configuration`
- `location elin-location`
- `show lldp interface`
- `switchport voice dscp`
- `switchport voice vlan`
- `switchport voice vlan priority`
**lldp non-strict-med-tlv-order-check**

**Overview**
Use this command to enable non-strict order checking for LLDP-MED advertisements it receives. That is, use this command to enable LLDP to receive and store TLVs from LLDP-MED advertisements even if they do not use standard TLV order.

Use the `no` variant of this command to disable non-strict order checking for LLDP-MED advertisements, that is, to set strict TLV order checking, so that LLDP discards any LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement.

**Syntax**
```
lldp non-strict-med-tlv-order-check
no lldp non-strict-med-tlv-order-check
```

**Default**
By default TLV non-strict order checking for LLDP-MED advertisements is disabled. That is, strict order checking is applied to LLDP-MED advertisements, according to ANSI/TIA-1057, and LLDP-MED TLVs in non-standard order are discarded.

**Mode**
Global Configuration

**Usage**
The ANSI/TIA-1057 specifies standard order for TLVs in LLDP-MED advertisements, and specifies that if LLDP receives LLDP advertisements with non-standard LLDP-MED TLV order, the TLVs in non-standard order should be discarded. This implementation of LLDP-MED follows the standard: it transmits TLVs in the standard order, and by default discards LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement. However, some implementations of LLDP transmit LLDP-MED advertisements with non-standard TLV order. To receive and store the data from these non-standard advertisements, enable non-strict order checking for LLDP-MED advertisements using this command.

**Examples**
To enable strict TLV order checking, use the commands:
```
awplus# configure terminal
awplus(config)# lldp tlv-order-check
```

To disable strict TLV order checking, use the commands:
```
awplus# configure terminal
awplus(config)# no lldp tlv-order-check
```

**Related Commands**
```
show running-config lldp
```
**lldp notification-interval**

**Overview**
This command sets the notification interval. This is the minimum interval between LLDP SNMP notifications (traps) of each kind (LLDP Remote Tables Change Notification and LLDP-MED Topology Change Notification).

The `no` variant of this command sets the notification interval back to its default.

**Syntax**
```
lldp notification-interval <5-3600>
no lldp notification-interval
```

**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
```

**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>
nolldp timer
```

**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)# nolldp timer
```

**Related Commands**

- `lldp tx-delay`
- `show lldp`
**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**

```plaintext
lldp tlv-select { [<tlv>]... }
lldp tlv-select all
no lldp tlv-select { [<tlv>]... }
no lldp tlv-select all
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;tlv&gt;</code></td>
<td>The TLV to transmit in LLDP advertisements. One of these keywords:</td>
</tr>
<tr>
<td></td>
<td>• port-description (specified by the <code>description (interface)</code> command)</td>
</tr>
<tr>
<td></td>
<td>• system-name (specified by the <code>hostname</code> command)</td>
</tr>
<tr>
<td></td>
<td>• system-description</td>
</tr>
<tr>
<td></td>
<td>• system-capabilities</td>
</tr>
<tr>
<td></td>
<td>• management-address</td>
</tr>
<tr>
<td></td>
<td>• port-vlan</td>
</tr>
<tr>
<td></td>
<td>• port-and-protocol-vlans</td>
</tr>
<tr>
<td></td>
<td>• vlan-names</td>
</tr>
<tr>
<td></td>
<td>• protocol-ids</td>
</tr>
<tr>
<td></td>
<td>• mac-phy-config</td>
</tr>
<tr>
<td></td>
<td>• power-management (Power Via MDI TLV)</td>
</tr>
<tr>
<td></td>
<td>• link-aggregation</td>
</tr>
<tr>
<td></td>
<td>• max-frame-size</td>
</tr>
<tr>
<td><code>all</code></td>
<td>All TLVs.</td>
</tr>
</tbody>
</table>

**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:

```bash
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:

```bash
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:

```bash
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:

```bash
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]}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>transmit</td>
<td>Enable or disable transmission of LLDP advertisements via this port or ports.</td>
</tr>
<tr>
<td>receive</td>
<td>Enable or disable reception of LLDP advertisements via this port or ports.</td>
</tr>
</tbody>
</table>

**Default**  
LLDP advertisement transmission and reception are enabled on all ports by default.

**Mode**  
Interface Configuration

**Examples**  
To enable transmission of LLDP advertisements on ports 1.0.1 and 1.0.6, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp transmit
```

To enable LLDP advertisement transmission and reception on ports 1.0.1 and 1.0.6, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp transmit receive
```

To disable LLDP advertisement transmission and reception on ports 1.0.1 and 1.0.6, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp transmit receive
```

**Related Commands**  
show lldp interface
**lldp tx-delay**

**Overview**
This command sets the value of the transmission delay timer. This is the minimum time interval between transmitting LLDP advertisements due to a change in LLDP local information.

The **no** variant of this command sets the transmission delay timer back to its default setting.

**Syntax**
```plaintext
lldp tx-delay <1-8192>
no lldp tx-delay
```

**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:
```plaintext
awplus# configure terminal
awplus(config)# lldp tx-delay 12
```

To set the transmission delay timer back to its default, use the commands:
```plaintext
awplus# configure terminal
awplus(config)# no lldp tx-delay
```

**Related Commands**
- `lldp timer`
- `show lldp`
**location civic-location configuration**

**Overview**  Use these commands to configure a civic address location. The country parameter must be specified first, and at least one of the other parameters must be configured before the location can be assigned to a port.

Use the `no` variants of this command to delete civic address parameters from the location.
Syntax

country <country>
state <state>
no state
county <county>
no county
city <city>
no city
division <division>
no division
neighborhood <neighborhood>
no neighborhood
street-group <street-group>
no street-group
leading-street-direction <leading-street-direction>
no leading-street-direction
trailing-street-suffix <trailing-street-suffix>
no trailing-street-suffix
street-suffix <street-suffix>
no street-suffix
house-number <house-number>
no house-number
house-number-suffix <house-number-suffix>
no house-number-suffix
landmark <landmark>
no landmark
additional-information <additional-information>
no additional-information
name <name>
no name
postalcode <postalcode>
no postalcode
building <building>
no building
unit <unit>
no unit
floor <floor>
no floor
room <room>
LLDP COMMANDS
LOCATION CIVIC-LOCATION CONFIGURATION

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;country&gt;</td>
<td>Upper-case two-letter country code, as specified in ISO 3166.</td>
</tr>
<tr>
<td>&lt;state&gt;</td>
<td>State (Civic Address (CA) Type 1): national subdivisions (state, canton, region).</td>
</tr>
<tr>
<td>&lt;county&gt;</td>
<td>County (CA Type 2): County, parish, gun (JP), district (IN).</td>
</tr>
<tr>
<td>&lt;city&gt;</td>
<td>City (CA Type 3): city, township, shi (JP).</td>
</tr>
<tr>
<td>&lt;division&gt;</td>
<td>City division (CA Type 4): City division, borough, city district, ward, chou (JP).</td>
</tr>
<tr>
<td>&lt;neighborhood&gt;</td>
<td>Neighborhood (CA Type 5): neighborhood, block.</td>
</tr>
<tr>
<td>&lt;street-group&gt;</td>
<td>Street group (CA Type 6): group of streets below the neighborhood level.</td>
</tr>
<tr>
<td>&lt;leading-street-direction&gt;</td>
<td>Leading street direction (CA Type 16).</td>
</tr>
</tbody>
</table>
## LLDP COMMANDS

### LOCATION CIVIC-LOCATION CONFIGURATION

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;trailing-street-suffix&gt;</td>
<td>Trailing street suffix (CA Type 17).</td>
</tr>
<tr>
<td>&lt;street-suffix&gt;</td>
<td>Street suffix (CA Type 18): street suffix or type.</td>
</tr>
<tr>
<td>&lt;house-number&gt;</td>
<td>House number (CA Type 19).</td>
</tr>
<tr>
<td>&lt;house-number-suffix&gt;</td>
<td>House number suffix (CA Type 20).</td>
</tr>
<tr>
<td>&lt;landmark&gt;</td>
<td>Landmark or vanity address (CA Type 21).</td>
</tr>
<tr>
<td>&lt;additional-information&gt;</td>
<td>Additional location information (CA Type 22).</td>
</tr>
<tr>
<td>&lt;name&gt;</td>
<td>Name (CA Type 23): residence and office occupant.</td>
</tr>
<tr>
<td>&lt;postal-code&gt;</td>
<td>Postal/zip code (CA Type 24).</td>
</tr>
<tr>
<td>&lt;building&gt;</td>
<td>Building (CA Type 25): structure.</td>
</tr>
<tr>
<td>&lt;unit&gt;</td>
<td>Unit (CA Type 26): apartment, suite.</td>
</tr>
<tr>
<td>&lt;floor&gt;</td>
<td>Floor (CA Type 27).</td>
</tr>
<tr>
<td>&lt;room&gt;</td>
<td>Room (CA Type 28).</td>
</tr>
<tr>
<td>&lt;place-type&gt;</td>
<td>Type of place (CA Type 29).</td>
</tr>
<tr>
<td>&lt;postal-community-name&gt;</td>
<td>Postal community name (CA Type 30).</td>
</tr>
<tr>
<td>&lt;post-office-box&gt;</td>
<td>Post office box (P.O. Box) (CA Type 31).</td>
</tr>
<tr>
<td>&lt;additional-code&gt;</td>
<td>Additional code (CA Type 32).</td>
</tr>
<tr>
<td>&lt;seat&gt;</td>
<td>Seat (CA Type 33): seat (desk, cubicle, workstation).</td>
</tr>
<tr>
<td>&lt;primary-road-name&gt;</td>
<td>Primary road name (CA Type 34).</td>
</tr>
<tr>
<td>&lt;road-section&gt;</td>
<td>Road section (CA Type 35).</td>
</tr>
<tr>
<td>&lt;branch-road-name&gt;</td>
<td>Branch road name (CA Type 36).</td>
</tr>
<tr>
<td>&lt;sub-branch-road-name&gt;</td>
<td>Sub-branch road name (CA Type 37).</td>
</tr>
<tr>
<td>&lt;street-name-pre-modifier&gt;</td>
<td>Street name pre-modifier (CA Type 38).</td>
</tr>
<tr>
<td>&lt;street-name-post-modifier&gt;</td>
<td>Street name post-modifier (CA Type 39).</td>
</tr>
</tbody>
</table>

### Default

By default no civic address location information is configured.

### Mode

Civic Address Location Configuration

### Usage

The **country** parameter must be configured before any other parameters can be configured; this creates the location. The country parameter cannot be deleted. One or more of the other parameters must be configured before the location can be assigned to a port. The country parameter must be entered as an upper-case two-letter country code, as specified in ISO 3166. All other parameters are entered as alpha-numeric strings. Do not configure all the civic address parameters (this would generate TLVs that are too long). Configure a subset of these
parameters—enough to consistently and precisely identify the location of the device. If the location is to be used for Emergency Call Service (ECS), the particular ECS application may have guidelines for configuring the civic address location. For more information about civic address format, see the LLDP Feature Overview and Configuration Guide.

To specify the civic address location, use the `location civic-location identifier` command. To delete the civic address location, use the `no` variant of the `location civic-location identifier` command. To assign the civic address location to particular ports, so that it can be advertised in TLVs from those ports, use the command `location civic-location-id` command.

**Examples**

To configure civic address location 1 with location "27 Nazareth Avenue, Christchurch, New Zealand" in civic-address format, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)# country NZ
awplus(config-civic)# city Christchurch
awplus(config-civic)# primary-road-name Nazareth
awplus(config-civic)# street-suffix Avenue
awplus(config-civic)# house-number 27
```

**Related Commands**

- `location civic-location-id`
- `location civic-location identifier`
- `show lldp local-info`
- `show location`
**location civic-location identifier**

**Overview**  Use this command to enter the Civic Address Location Configuration mode to configure the specified location.

Use the **no** variant of this command to delete a civic address location. This also removes the location from any ports it has been assigned to.

**Syntax**

```
location civic-location identifier <civic-loc-id>
```

```
no location civic-location identifier <civic-loc-id>
```

**Default**  By default there are no civic address locations.

**Mode**  Global Configuration

**Usage**  To configure the location information for this civic address location identifier, use the `location civic-location configuration` command. To associate this civic location identifier with particular ports, use the `location elin-location-id` command.

Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

**Examples**  To enter Civic Address Location Configuration mode for the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)#
```

To delete the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location civic-location identifier 1
```

**Related Commands**

- `location civic-location-id`
- `location civic-location configuration`
- `show location`
- `show running-config lldp`
**location civic-location-id**

**Overview**  Use this command to assign a civic address location to the ports. The civic address location must already exist. This replaces any previous assignment of civic address location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location identifier from the ports.

**Syntax**

```
location civic-location-id <civic-loc-id>
no location civic-location-id [<civic-loc-id>]
```

**Default**  By default no civic address location is assigned to ports.

**Mode**  Interface Configuration

**Usage**  The civic address location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, create the location using the following commands:

- `location civic-location identifier` command
- `location civic-location configuration` command

If a civic-address location is deleted using the **no** variant of the `location civic-location identifier` command, it is automatically removed from all ports.

**Examples**

To assign the civic address location 1 to port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location civic-location-id 1
```

To remove a civic address location from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location civic-location-id
```

**Related Commands**

- `lldp med-tlv-select`
- `location civic-location identifier`
- `location civic-location configuration`
- `show location`
LLDP COMMANDS
LOCATION COORD-LOCATION CONFIGURATION

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**

```plaintext
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}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;lat-resolution&gt;</td>
<td>Latitude resolution, as a number of valid bits, in the range 0 to 34.</td>
</tr>
<tr>
<td>&lt;latitude&gt;</td>
<td>Latitude value in degrees in the range -90.0 to 90.0</td>
</tr>
<tr>
<td>&lt;long-resolution&gt;</td>
<td>Longitude resolution, as a number of valid bits, in the range 0 to 34.</td>
</tr>
<tr>
<td>&lt;longitude&gt;</td>
<td>Longitude value in degrees, in the range -180.0 to 180.0.</td>
</tr>
<tr>
<td>&lt;alt-resolution&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;altitude&gt;</td>
<td>Altitude value, in meters or floors.</td>
</tr>
<tr>
<td>meters</td>
<td>The altitude value is in meters.</td>
</tr>
<tr>
<td>floors</td>
<td>The altitude value is in floors.</td>
</tr>
<tr>
<td>datum</td>
<td>The geodetic system (or datum) that the specified coordinate values are based on.</td>
</tr>
<tr>
<td>wgs84</td>
<td>World Geodetic System 1984.</td>
</tr>
</tbody>
</table>

**Default**
By default no coordinate location information is configured.

**Mode**
Coordinate Configuration

**Usage**
Latitude and longitude values are always stored internally, and advertised in the Location Identification TLV, as 34-bit fixed-point binary numbers, with a 25-bit fractional part, irrespective of the number of digits entered by the user. Likewise
altitude is stored as a 30-bit fixed point binary number, with an 8-bit fractional part. Because the user-entered decimal values are stored as fixed point binary numbers, they cannot always be represented exactly—the stored binary number is converted to a decimal number for display in the output of the show location command. For example, a user-entered latitude value of “2.77” degrees is displayed as “2.7699999809265136718750000”.

The `lat-resolution`, `long-resolution`, and `alt-resolution` parameters allow the user to specify the resolution of each coordinate element as the number of valid bits in the internally-stored binary representation of the value. These resolution values can be used by emergency services to define a search area.

To specify the coordinate identifier, use the `location coord-location identifier` command. To remove coordinate information, delete the coordinate location by using the `no` variant of that command. To associate the coordinate location with particular ports, so that it can be advertised in TLVs from those ports, use the `location elin-location-id` command.

**Example**

To configure the location for the White House in Washington DC, which has the coordinates based on the WGS84 datum of 38.89868 degrees North (with 22 bit resolution), 77.03723 degrees West (with 22 bit resolution), and 15 meters height (with 9 bit resolution), use the commands:

```
awplus# configure terminal
awplus(config)# location coord-location identifier 1
awplus(config-coord)# la-resolution 22
awplus(config-coord)# latitude 38.89868
awplus(config-coord)# lo-resolution 22
awplus(config-coord)# longitude -77.03723
awplus(config-coord)# alt-resolution 9
awplus(config-coord)# altitude 15 meters
awplus(config-coord)# datum wgs84
```

**Related Commands**

- `location coord-location-id`
- `location coord-location identifier`
- `show lldp local-info`
- `show location`
location coord-location identifier

**Overview**
Use this command to enter Coordinate Location Configuration mode for this coordinate location.

Use the **no** variant of this command to delete a coordinate location. This also removes the location from any ports it has been assigned to.

**Syntax**
```
location coord-location identifier <coord-loc-id>
no location coord-location identifier <coord-loc-id>
```

**Parameter** | **Description**
---|---
<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

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>]
```

**Default**
By default no coordinate location is assigned to ports.

**Mode**
Interface Configuration

**Usage**
The coordinate location associated with a port can be transmitted in Location
Identification TLVs via the port.

Before using this command, configure the location using the following
commands:

- location coord-location identifier command
- location coord-location configuration command

If a coordinate location is deleted using the **no** variant of the location
cord-location identifier command, it is automatically removed from all ports.

**Examples**
To assign coordinate location 1 to port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location coord-location-id 1
```

To remove a coordinate location from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location coord-location-id
```

**Related Commands**
lldp med-tlv-select
location coord-location identifier
location coord-location configuration
show location
**location elin-location**

**Overview**  Use this command to create or modify an ELIN location. Use the `no` variant of this command to delete an ELIN location, and remove it from any ports it has been assigned to.

**Syntax**  

```
location elin-location <elin> identifier <elin-loc-id>
nolocation elin-location identifier <elin-loc-id>
```

**Parameter**  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;elin&gt;</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;elin-loc-id&gt;</code></td>
<td>A unique ELIN location identifier, in the range 1 to 4095.</td>
</tr>
</tbody>
</table>

**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_>]
```

**Default**  By default no ELIN location is assigned to ports.

**Mode**  Interface Configuration

**Usage**  An ELIN location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, configure the location using the `location elin-location` command.

If an ELIN location is deleted using the **no** variant of one of the `location elin-location` command, it is automatically removed from all ports.

**Examples**

To assign ELIN location 1 to port 1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location elin-location-id 1
```

To remove an ELIN location from port 1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location elin-location-id
```

**Related Commands**

- `lldp med-tlv-select`
- `location elin-location`
- `show location`
show debugging lldp

**Overview**  This command displays LLDP debug settings for specified ports. If no port list is supplied, LLDP debug settings for all ports are displayed.

**Syntax**  `show debugging lldp [interface <port-list>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports for which the LLDP debug settings are shown.</td>
</tr>
</tbody>
</table>

**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 50-1: 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 50-1:** Parameters in the output of the `show debugging lldp` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port name.</td>
</tr>
<tr>
<td>Rx</td>
<td>Whether debugging of LLDP receive is enabled on the port.</td>
</tr>
<tr>
<td>RxPkt</td>
<td>Whether debugging of LLDP receive packet dump is enabled on the port.</td>
</tr>
<tr>
<td>Tx</td>
<td>Whether debugging of LLDP transmit is enabled on the port.</td>
</tr>
<tr>
<td>TxPkt</td>
<td>Whether debugging of LLDP transmit packet dump is enabled on the port.</td>
</tr>
</tbody>
</table>
LLDP COMMANDS
SHOW DEBUGGING LLDP

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 50-2: 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 50-3: Parameters in the output of the **show lldp** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP Status</td>
<td>Whether LLDP is enabled. Default is disabled.</td>
</tr>
<tr>
<td>Notification Interval</td>
<td>Minimum interval between LLDP notifications.</td>
</tr>
<tr>
<td>Tx Timer Interval</td>
<td>Transmit interval between regular transmissions of LLDP advertisements.</td>
</tr>
<tr>
<td>Hold-time Multiplier</td>
<td>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.</td>
</tr>
<tr>
<td>Reinitialization Delay</td>
<td>The reinitialization delay. This is the minimum time after disabling LLDP transmit on a port before it can reinitialize again.</td>
</tr>
</tbody>
</table>
Table 50-3: Parameters in the output of the `show lldp` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Delay</td>
<td>The transmission delay. This is the minimum time interval between transmitting advertisements due to a change in LLDP local information.</td>
</tr>
<tr>
<td>Port Number Type</td>
<td>The type of port identifier used to enumerate LLDP MIB local port entries, as set by the <code>lldp port-number-type</code> command.</td>
</tr>
<tr>
<td>Fast Start Count</td>
<td>The number of times fast start advertisements are sent for LLDP-MED.</td>
</tr>
<tr>
<td>Total Neighbor Count</td>
<td>Number of LLDP neighbors discovered on all ports.</td>
</tr>
<tr>
<td>Neighbors table last updated</td>
<td>The time since the LLDP neighbor table was last updated.</td>
</tr>
</tbody>
</table>

**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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports for which the LLDP configuration settings are to be shown.</td>
</tr>
</tbody>
</table>

**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 50-2:  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

<table>
<thead>
<tr>
<th>Port</th>
<th>Rx/Tx</th>
<th>Notif</th>
<th>Management Addr</th>
<th>Base</th>
<th>802.1</th>
<th>802.3</th>
<th>MED</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.1</td>
<td>Rx</td>
<td>TX</td>
<td>RC --</td>
<td>192.168.100.123</td>
<td>PdSnSdScMa</td>
<td>--------</td>
<td>McNLoPe---</td>
</tr>
<tr>
<td>*1.0.2</td>
<td></td>
<td></td>
<td>--</td>
<td>192.168.100.123</td>
<td>PdSnSdScMa</td>
<td>--------</td>
<td>McNLoPe---</td>
</tr>
<tr>
<td>1.0.3</td>
<td>Rx</td>
<td>RC</td>
<td>--</td>
<td>192.168.100.123</td>
<td>Pd--SdScMa</td>
<td>PVPpVnPi</td>
<td>McNLoPe---</td>
</tr>
<tr>
<td>1.0.4</td>
<td></td>
<td></td>
<td>RC</td>
<td>192.168.100.123</td>
<td>PdSnSd--Ma</td>
<td>--------</td>
<td>McNLoPe---</td>
</tr>
<tr>
<td>1.0.5</td>
<td>Rx</td>
<td>TX</td>
<td>RC TC</td>
<td>192.168.100.123</td>
<td>PdSnSdScMa</td>
<td>PVPpVnPi</td>
<td>McNLoPe---</td>
</tr>
<tr>
<td>1.0.6</td>
<td>Rx</td>
<td>TX</td>
<td>RC TC</td>
<td>192.168.100.123</td>
<td>Pd---ScMa</td>
<td>--------</td>
<td>McNLoPe---</td>
</tr>
<tr>
<td>1.0.7</td>
<td>Rx</td>
<td>--</td>
<td>TC</td>
<td>192.168.100.123</td>
<td>PdSnSdScMa</td>
<td>PVPpVnPi</td>
<td>MPPoLaMf</td>
</tr>
<tr>
<td>1.0.8</td>
<td>Rx</td>
<td>--</td>
<td>TC</td>
<td>192.168.1.1</td>
<td>PdSn--ScMa</td>
<td>PVPpVnPi</td>
<td>McNp--------</td>
</tr>
</tbody>
</table>
```
**Table 50-4: Parameters in the output of the **show lldp interface** command**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port name.</td>
</tr>
<tr>
<td>Rx</td>
<td>Whether reception of LLDP advertisements is enabled on the port.</td>
</tr>
<tr>
<td>Tx</td>
<td>Whether transmission of LLDP advertisements is enabled on the port.</td>
</tr>
<tr>
<td>Notif</td>
<td>Whether sending SNMP notification for LLDP is enabled on the port:</td>
</tr>
<tr>
<td>Management Addr</td>
<td>Management address advertised to neighbors.</td>
</tr>
<tr>
<td>Base TLVs Enabled for Tx</td>
<td>List of optional Base TLVs enabled for transmission:</td>
</tr>
<tr>
<td>802.1 TLVs Enabled for Tx</td>
<td>List of optional 802.1 TLVs enabled for transmission:</td>
</tr>
<tr>
<td>802.3 TLVs Enabled for Tx</td>
<td>List of optional 802.3 TLVs enabled for transmission:</td>
</tr>
<tr>
<td>MED TLVs Enabled for Tx</td>
<td>List of optional LLDP-MED TLVs enabled for transmission:</td>
</tr>
</tbody>
</table>

**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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>Information for base TLVs.</td>
</tr>
<tr>
<td>dot1</td>
<td>Information for 802.1 TLVs.</td>
</tr>
<tr>
<td>dot3</td>
<td>Information for 802.3 TLVs.</td>
</tr>
<tr>
<td>med</td>
<td>Information for LLDP-MED TLVs.</td>
</tr>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports for which the local information is to be shown.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Usage**  Whether and which local information is transmitted in advertisements via a port depends on:

- whether the port is set to transmit LLDP advertisements (`lldp transmit receive` command)
- which TLVs it is configured to send (`lldp tlv-select` command, `lldp med-tlv-select` command)

**Examples**  To display local information transmitted via port 1.0.1, use the command:
```
awplus# show lldp local-info interface port1.0.1
```
To display local information transmitted via all ports, use the command:
```
awplus# show lldp local-info
```
LLDP LOCAL INFORMATION

Output  Figure 50-3: Example output from show lldp local-info

<table>
<thead>
<tr>
<th>LLDP Local Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local port1.0.1:</td>
</tr>
<tr>
<td>Chassis ID Type ..........</td>
</tr>
<tr>
<td>Chassis ID ..............</td>
</tr>
<tr>
<td>Port ID Type ............</td>
</tr>
<tr>
<td>Port ID ..................</td>
</tr>
<tr>
<td>TTL ........................</td>
</tr>
<tr>
<td>Port Description ..........</td>
</tr>
<tr>
<td>System Name .............</td>
</tr>
<tr>
<td>System Description ........</td>
</tr>
<tr>
<td>System Capabilities - Supported ..</td>
</tr>
<tr>
<td>- Enabled .... Bridge, Router</td>
</tr>
<tr>
<td>Management Address ..........</td>
</tr>
<tr>
<td>Port VLAN ID (PVID) .......</td>
</tr>
<tr>
<td>Port &amp; Protocol VLAN - Supported .</td>
</tr>
<tr>
<td>- Enabled ... No</td>
</tr>
<tr>
<td>- VIDs ...... 0</td>
</tr>
<tr>
<td>VLAN Names ..................</td>
</tr>
<tr>
<td>Protocol IDs ..............</td>
</tr>
<tr>
<td>MAC/PHY Auto-negotiation .......</td>
</tr>
<tr>
<td>Advertised Capability ......</td>
</tr>
<tr>
<td>Operational MAU Type ........</td>
</tr>
<tr>
<td>Power Via MDI (PoE) ..........</td>
</tr>
<tr>
<td>Port Class .............. PSE</td>
</tr>
<tr>
<td>Pair Control Ability ......</td>
</tr>
<tr>
<td>Power Class ............ Unknown</td>
</tr>
<tr>
<td>Link Aggregation ..........</td>
</tr>
<tr>
<td>Maximum Frame Size .........</td>
</tr>
<tr>
<td>LLDP-MED Device Type ........</td>
</tr>
<tr>
<td>LLDP-MED Capabilities ........</td>
</tr>
<tr>
<td>Network Policy ...........</td>
</tr>
<tr>
<td>Location Identification ....</td>
</tr>
<tr>
<td>Country Code ............ NZ</td>
</tr>
<tr>
<td>City ...................... Christchurch</td>
</tr>
<tr>
<td>Street Suffix ............ Avenue</td>
</tr>
<tr>
<td>House Number ............ 27</td>
</tr>
<tr>
<td>Primary Road Name ........ Nazareth</td>
</tr>
<tr>
<td>Location Identification ....</td>
</tr>
<tr>
<td>ELIN ........................</td>
</tr>
<tr>
<td>Extended Power Via MDI (PoE) ....</td>
</tr>
<tr>
<td>Power Source ............ Primary Power</td>
</tr>
<tr>
<td>Power Priority ........... Low</td>
</tr>
<tr>
<td>Power Value ............ 4.4 Watts</td>
</tr>
</tbody>
</table>

Inventory Management:
Hardware Revision ........ A-0
Firmware Revision .......... 1.1.0
Software Revision .......... v5.4.3A
Serial Number .............. G1Q78900B
Manufacturer Name .......... Allied Telesis Inc.
Model Name .................. x610-48Ts/XP
Asset ID ................... [zero length]
### Table 50-5: Parameters in the output of `show lldp local-info`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis ID Type</td>
<td>Type of the Chassis ID.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Chassis ID that uniquely identifies the local device.</td>
</tr>
<tr>
<td>Port ID Type</td>
<td>Type of the Port ID.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Port ID of the local port through which advertisements are sent.</td>
</tr>
<tr>
<td>TTL</td>
<td>Number of seconds that the information advertised by the local port remains valid.</td>
</tr>
<tr>
<td>Port Description</td>
<td>Port description of the local port, as specified by the <code>description (interface)</code> command.</td>
</tr>
<tr>
<td>System Name</td>
<td>System name, as specified by the <code>hostname</code> command.</td>
</tr>
<tr>
<td>System Description</td>
<td>System description.</td>
</tr>
<tr>
<td>System Capabilities (Supported)</td>
<td>Capabilities that the local port supports.</td>
</tr>
<tr>
<td>System Capabilities (Enabled)</td>
<td>Enabled capabilities on the local port.</td>
</tr>
<tr>
<td>Management Addresses</td>
<td>Management address associated with the local port. To change this, use the <code>lldp management-address</code> command.</td>
</tr>
<tr>
<td>Port VLAN ID (PVID)</td>
<td>VLAN identifier associated with untagged or priority tagged frames received via the local port.</td>
</tr>
<tr>
<td>Port &amp; Protocol VLAN (Supported)</td>
<td>Whether Port &amp; Protocol VLANs (PPV) is supported on the local port.</td>
</tr>
<tr>
<td>Port &amp; Protocol VLAN (Enabled)</td>
<td>Whether the port is in one or more Port &amp; Protocol VLANs.</td>
</tr>
<tr>
<td>Port &amp; Protocol VLAN (VIDs)</td>
<td>List of identifiers for Port &amp; Protocol VLANs that the port is in.</td>
</tr>
<tr>
<td>VLAN Names</td>
<td>List of VLAN names for VLANs that the local port is assigned to.</td>
</tr>
<tr>
<td>Protocol IDs</td>
<td>List of protocols that are accessible through the local port.</td>
</tr>
<tr>
<td>MAC/PHY Auto-negotiation</td>
<td>Auto-negotiation support and current status of the 802.3 LAN on the local port.</td>
</tr>
</tbody>
</table>
### LLDP COMMANDS

#### SHOW LLDP LOCAL-INFO

The following table lists the parameters that can be configured using the `show lldp local-info` command in **AlliedWare Plus™ Operating System - Version 5.4.5-0.x**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Via MDI (PoE)</td>
<td>PoE-capability and current status on the local port.</td>
</tr>
<tr>
<td>Port Class</td>
<td>Whether the device is a PSE (Power Sourcing Entity) or a PD (Powered Device)</td>
</tr>
<tr>
<td>Pair Control Ability</td>
<td>Whether power pair selection can be controlled</td>
</tr>
<tr>
<td>Power Pairs</td>
<td>Which power pairs are selected for power (&quot;Signal Pairs&quot; or &quot;Spare Pairs&quot;) if pair selection can be controlled</td>
</tr>
<tr>
<td>Power Class</td>
<td>The power class of the PD device on the port (class 0, 1, 2, 3 or 4)</td>
</tr>
<tr>
<td>Link Aggregation</td>
<td>Whether the link is capable of being aggregated and it is currently in an aggregation.</td>
</tr>
<tr>
<td>Aggregated Port-ID</td>
<td>Aggregated port identifier.</td>
</tr>
<tr>
<td>Maximum Frame Size</td>
<td>The maximum frame size capability of the implemented MAC and PHY.</td>
</tr>
<tr>
<td>LLDP-MED Device Type</td>
<td>LLDP-MED device type</td>
</tr>
<tr>
<td>LLDP-MED Capabilities</td>
<td>Capabilities LLDP-MED capabilities supported on the local port.</td>
</tr>
<tr>
<td>Network Policy</td>
<td>List of network policies configured on the local port.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN identifier for the port for the specified application type</td>
</tr>
<tr>
<td>Tagged Flag</td>
<td>Whether the VLAN ID is to be used as tagged or untagged</td>
</tr>
<tr>
<td>Layer-2 Priority:</td>
<td>Layer 2 User Priority (in the range 0 to 7)</td>
</tr>
<tr>
<td>DSCP Value</td>
<td>Diffserv codepoint (in the range 0 to 63)</td>
</tr>
<tr>
<td>Location Identification</td>
<td>Location configured on the local port.</td>
</tr>
<tr>
<td>Extended Power Via MDI (PoE)</td>
<td>PoE-capability and current status of the PoE parameters for Extended Power-Via-MDI TLV on the local port.</td>
</tr>
<tr>
<td>Power Source</td>
<td>The power source the switch currently uses; either primary power or backup power.</td>
</tr>
<tr>
<td>Power Priority</td>
<td>The power priority configured on the port; either critical, high or low.</td>
</tr>
</tbody>
</table>
### Table 50-5: Parameters in the output of `show lldp local-info` (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Value</td>
<td>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.</td>
</tr>
<tr>
<td>Inventory Management</td>
<td>Inventory information for the device.</td>
</tr>
</tbody>
</table>

**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>]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;port-list&gt;</code></td>
<td>The ports for which the neighbor information is to be shown.</td>
</tr>
</tbody>
</table>

**Mode**  User Exec and Privileged Exec

**Examples**  To display neighbor information received via all ports, use the command:

```plaintext
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:

```plaintext
awplus# show lldp neighbors interface port1.0.1,port1.0.6
```

**Output**  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

<table>
<thead>
<tr>
<th>Local Port</th>
<th>Neighbor Chassis ID</th>
<th>Neighbor Port ID</th>
<th>Neighbor Sys Name</th>
<th>Neighbor Cap.</th>
<th>Neighbor Ty Pwr</th>
<th>System</th>
<th>MED</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.1</td>
<td>002d.3044.7ba6</td>
<td>port1.0.2</td>
<td>awplus</td>
<td>OPBWRTCS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.1</td>
<td>0011.3109.e5c6</td>
<td>port1.0.3</td>
<td>AT-9924 switch/route...</td>
<td>--B-R---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.6</td>
<td>0000.10cf.8590</td>
<td>port3</td>
<td>AR-442S</td>
<td>--B-R---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.6</td>
<td>00ee.4352.df51</td>
<td>192.168.1.2</td>
<td>Jim’s desk phone</td>
<td>--B--T--</td>
<td>3 PSE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Table 50-6: Parameters in the output of the `show lldp neighbors` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Port</td>
<td>Local port on which the neighbor information was received.</td>
</tr>
<tr>
<td>Neighbor Chassis ID</td>
<td>Chassis ID that uniquely identifies the neighbor.</td>
</tr>
</tbody>
</table>
### Table 50-6: Parameters in the output of the `show lldp neighbors` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Port Name</td>
<td>Port ID of the neighbor.</td>
</tr>
<tr>
<td>Neighbor Sys Name</td>
<td>System name of the LLDP neighbor.</td>
</tr>
<tr>
<td>Neighbor Capability</td>
<td>Capabilities that are supported and enabled on the neighbor.</td>
</tr>
<tr>
<td>System Capability</td>
<td>System Capabilities of the LLDP neighbor.</td>
</tr>
<tr>
<td>MED Device Type</td>
<td>LLDP-MED Device class (Class I, II, III or Network Connectivity)</td>
</tr>
<tr>
<td>MED Power Source</td>
<td>LLDP-MED Power Source</td>
</tr>
</tbody>
</table>

**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>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>Information for base TLVs.</td>
</tr>
<tr>
<td>dot1</td>
<td>Information for 802.1 TLVs.</td>
</tr>
<tr>
<td>dot3</td>
<td>Information for 803.1 TLVs.</td>
</tr>
<tr>
<td>med</td>
<td>Information for LLDP-MED TLVs.</td>
</tr>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports for which the neighbor information is to be shown.</td>
</tr>
</tbody>
</table>

**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 50-5: Example output from the `show lldp neighbors detail` command

```bash
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+ v5.4.4
- 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 ...... 1000BaseT, 100BaseTXFD, 100BaseTX,
    10BaseT, 10BaseTFD
- 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 ........ v5.4.4
  - Serial Number ........... M1NB73008
  - Manufacturer Name ........ Allied Telesis Inc.
  - Model Name .............. SBx908
  - Asset ID ................ [zero length]
```
### Table 50-7: Parameters in the output of the `show lldp neighbors detail` command

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis ID Type</td>
<td>Type of the Chassis ID.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Chassis ID that uniquely identifies the neighbor.</td>
</tr>
<tr>
<td>Port ID Type</td>
<td>Type of the Port ID.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Port ID of the neighbor.</td>
</tr>
<tr>
<td>TTL</td>
<td>Number of seconds that the information advertised by the neighbor remains valid.</td>
</tr>
<tr>
<td>Port Description</td>
<td>Port description of the neighbor’s port.</td>
</tr>
<tr>
<td>System Name</td>
<td>Neighbor’s system name.</td>
</tr>
<tr>
<td>System Description</td>
<td>Neighbor’s system description.</td>
</tr>
<tr>
<td>System Capabilities (Supported)</td>
<td>Capabilities that the neighbor supports.</td>
</tr>
<tr>
<td>System Capabilities (Enabled)</td>
<td>Capabilities that are enabled on the neighbor.</td>
</tr>
<tr>
<td>Management Addresses</td>
<td>List of neighbor’s management addresses.</td>
</tr>
<tr>
<td>Port VLAN ID (PVID)</td>
<td>VLAN identifier associated with untagged or priority tagged frames for the neighbor port.</td>
</tr>
<tr>
<td>Port &amp; Protocol VLAN (Supported)</td>
<td>Whether Port &amp; Protocol VLAN is supported on the LLDP neighbor.</td>
</tr>
<tr>
<td>Port &amp; Protocol VLAN (Enabled)</td>
<td>Whether Port &amp; Protocol VLAN is enabled on the LLDP neighbor.</td>
</tr>
<tr>
<td>Port &amp; Protocol VLAN (VIDs)</td>
<td>List of Port &amp; Protocol VLAN identifiers.</td>
</tr>
<tr>
<td>VLAN Names</td>
<td>List of names of VLANs that the neighbor’s port belongs to.</td>
</tr>
<tr>
<td>Protocol IDs</td>
<td>List of protocols that are accessible through the neighbor’s port.</td>
</tr>
<tr>
<td>MAC/PHY Auto-negotiation</td>
<td>Auto-negotiation configuration and status</td>
</tr>
<tr>
<td>Power Via MDI (PoE)</td>
<td>PoE configuration and status of 802.3 Power-Via-MDI TLV</td>
</tr>
<tr>
<td>Link Aggregation</td>
<td>Link aggregation information</td>
</tr>
<tr>
<td>Maximum Frame Size</td>
<td>The maximum frame size capability</td>
</tr>
</tbody>
</table>
Table 50-7: Parameters in the output of the `show lldp neighbors detail` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP-MED Device Type</td>
<td>LLDP-MED Device type</td>
</tr>
<tr>
<td>LLDP-MED Capabilities</td>
<td>LLDP-MED capabilities supported</td>
</tr>
<tr>
<td>Network Policy</td>
<td>List of network policies</td>
</tr>
<tr>
<td>Location Identification</td>
<td>Location information</td>
</tr>
<tr>
<td>Extended Power Via MDI (PoE)</td>
<td>PoE-capability and current status</td>
</tr>
<tr>
<td>Inventory Management</td>
<td>Inventory information</td>
</tr>
</tbody>
</table>

**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 50-8: Example output from the *show lldp statistics* command

```
awplus# show lldp statistics
Global LLDP Packet and Event counters:
Frames: Out .......................... 345
       In .......................... 423
       In Errored .................. 0
       In Dropped ................. 0
TLVs: Unrecognized ............... 0
      Discarded .................. 0
Neighbors: New Entries .......... 20
          Deleted Entries ...... 20
          Dropped Entries ...... 0
          Entry Age-outs ........ 20
```

Table 50-9: Parameters in the output of the *show lldp statistics* command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frames Out</td>
<td>Number of LLDPDU frames transmitted.</td>
</tr>
<tr>
<td>Frames In</td>
<td>Number of LLDPDU frames received.</td>
</tr>
<tr>
<td>Frames In Errored</td>
<td>Number of invalid LLDPDU frames received.</td>
</tr>
<tr>
<td>Frames In Dropped</td>
<td>Number of LLDPDU frames received and discarded for any reason.</td>
</tr>
<tr>
<td>TLVs Unrecognized</td>
<td>Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types.</td>
</tr>
<tr>
<td>TLVs Discarded</td>
<td>Number of LLDP TLVs discarded for any reason.</td>
</tr>
<tr>
<td>Neighbors New Entries</td>
<td>Number of times the information advertised by neighbors has been inserted into the neighbor table.</td>
</tr>
<tr>
<td>Neighbors Deleted Entries</td>
<td>Number of times the information advertised by neighbors has been removed from the neighbor table.</td>
</tr>
</tbody>
</table>
Table 50-9: Parameters in the output of the `show lldp statistics` command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbors Dropped Entries</td>
<td>Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.</td>
</tr>
<tr>
<td>Neighbors Entry Age-outs Entries</td>
<td>Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired.</td>
</tr>
</tbody>
</table>

**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>]
```

**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 50-10: Example output from the **show lldp statistics interface** command

```
awplus# show lldp statistics interface port1.0.1,port1.0.6

LLDP Packet and Event Counters:

port1.0.1
Frames:  Out ................... 27
In .................... 22
In Errored ............ 0
In Dropped ............ 0
TLVs:  Unrecognized .......... 0
Discarded ............. 0
Neighbors:  New Entries ........... 3
Deleted Entries ....... 0
Dropped Entries ....... 0
Entry Age-outs ........ 0

port1.0.6
Frames:  Out ................... 15
In .................... 18
In Errored ............ 0
In Dropped ............ 0
TLVs:  Unrecognized .......... 0
Discarded ............. 0
Neighbors:  New Entries ........... 1
Deleted Entries ....... 0
Dropped Entries ....... 0
Entry Age-outs ........ 0
```
### Table 50-11: Parameters in the output of the `show lldp statistics interface` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frames Out</td>
<td>Number of LLDPDU frames transmitted.</td>
</tr>
<tr>
<td>Frames In</td>
<td>Number of LLDPDU frames received.</td>
</tr>
<tr>
<td>Frames In Errored</td>
<td>Number of invalid LLDPDU frames received.</td>
</tr>
<tr>
<td>Frames In Dropped</td>
<td>Number of LLDPDU frames received and discarded for any reason.</td>
</tr>
<tr>
<td>TLVs Unrecognized</td>
<td>Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types.</td>
</tr>
<tr>
<td>TLVs Discarded</td>
<td>Number of LLDP TLVs discarded for any reason.</td>
</tr>
<tr>
<td>Neighbors New Entries</td>
<td>Number of times the information advertised by neighbors has been inserted into the neighbor table.</td>
</tr>
<tr>
<td>Neighbors Deleted Entries</td>
<td>Number of times the information advertised by neighbors has been removed from the neighbor table.</td>
</tr>
<tr>
<td>Neighbors Dropped Entries</td>
<td>Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.</td>
</tr>
<tr>
<td>Neighbors Entry Age-outs Entries</td>
<td>Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired.</td>
</tr>
</tbody>
</table>

**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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>civic-location</td>
<td>Display civic location information.</td>
</tr>
<tr>
<td>coord-location</td>
<td>Display coordinate location information.</td>
</tr>
<tr>
<td>elin-location</td>
<td>Display ELIN location information.</td>
</tr>
<tr>
<td>&lt;civic-loc-id&gt;</td>
<td>Civic address location identifier, in the range 1 to 4095.</td>
</tr>
<tr>
<td>&lt;coord-loc-id&gt;</td>
<td>Coordinate location identifier, in the range 1 to 4095.</td>
</tr>
<tr>
<td>&lt;elin-loc-id&gt;</td>
<td>ELIN location identifier, in the range 1 to 4095.</td>
</tr>
<tr>
<td>&lt;port-list&gt;</td>
<td>Ports to display information about.</td>
</tr>
</tbody>
</table>

**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 50-12: Example output from the **show location** command

```
awplus# show location civic-location interface port1.0.1
Port  ID | Element Type | Element Value
---------|--------------|----------------
1.0.1    | 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
```
LLDP COMMANDS

SHOW LOCATION

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 50-13: Example output from the `show location` command

<table>
<thead>
<tr>
<th>ID</th>
<th>Element Type</th>
<th>Element Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Latitude Resolution</td>
<td>15 bits</td>
</tr>
<tr>
<td></td>
<td>Latitude</td>
<td>38.896481130123138427734375 degrees</td>
</tr>
<tr>
<td></td>
<td>Longitude Resolution</td>
<td>15 bits</td>
</tr>
<tr>
<td></td>
<td>Longitude</td>
<td>130.23232293128967285156250 degrees</td>
</tr>
<tr>
<td></td>
<td>Altitude Resolution</td>
<td>10 bits</td>
</tr>
<tr>
<td></td>
<td>Altitude</td>
<td>2.50000000 meters</td>
</tr>
<tr>
<td></td>
<td>Map Datum</td>
<td>WGS 84</td>
</tr>
</tbody>
</table>

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 50-14: Example output from the `show location elin-location` command

<table>
<thead>
<tr>
<th>ID</th>
<th>ELIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1234567890</td>
</tr>
<tr>
<td>2</td>
<td>5432154321</td>
</tr>
</tbody>
</table>

**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
Introduction

Overview  This chapter provides an alphabetical reference for commands used to configure SMTP.
For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Command List  

•  “debug mail” on page 2225
•  “delete mail” on page 2226
•  “mail” on page 2227
•  “mail from” on page 2228
•  “mail smtpserver” on page 2229
•  “show counter mail” on page 2230
•  “show mail” on page 2231
•  “undebug mail” on page 2232
debug mail

**Overview**  This command turns on debugging for sending emails. The **no** variant of this command turns off debugging for sending emails.

**Syntax**
- `debug mail`
- `no debug mail`

**Mode**  Privileged Exec

**Examples**
- To turn on debugging for sending emails, use the command:
  ```
  awplus# debug mail
  ```
- To turn off debugging for sending emails, use the command:
  ```
  awplus# no debug mail
  ```

**Related Commands**
- delete mail
- mail
- mail from
- mail smtpserver
- show mail
- show counter mail
- unddebug mail
delete mail

**Overview**  
This command deletes mail from the queue.

**Syntax**  
delete mail [mail-id <mail-id>|all]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail-id</td>
<td>Deletes a single mail from the mail queue.</td>
</tr>
<tr>
<td>&lt;mail-id&gt;</td>
<td>An unique mail ID number. Use the show mail command to display this for an item of mail.</td>
</tr>
<tr>
<td>all</td>
<td>Delete all the mail in the queue.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec

**Examples**  
To delete a unique mail item 20060912142356.1234 from the queue, use the command:

awplus# delete mail 20060912142356.1234

To delete all mail from the queue, use the command:

awplus# delete mail all

**Related Commands**  
debug mail
mail
mail from
mail smtpserver
show mail
mail

Overview
This command sends an email using the SMTP protocol. If you specify a file the text inside the file is sent in the message body.

If you do not specify the to, file, or subject parameters, the CLI prompts you for the missing information.

Before you can send mail using this command, you must specify the sending email address using the mail from command and a mail server using the mail smtpserver command.

Syntax
mail [{to <to>|subject <subject>|file <filename>}]

Parameter | Description
--- | ---
to | The email recipient.
<to> | Email address.
subject | Description of the subject of this email. Use quote marks when the subject text contains spaces.
<subject> | String.
file | File to insert as text into the message body.
<filename> | String.

Mode
Privileged Exec

Example
To send an email to rei@nerv.com with the subject dummy plug configuration, and with the message body inserted from the file plug.conf use the command:

awplus# mail rei@nerv.com subject dummy plug configuration filename plug.conf

Related Commands
debug mail
delete mail
mail from
mail smtpserver
show mail
show counter mail
**Overview**  This command sets an email address for the “mail from” SMTP command. You must specify a sending email address with this command before you can send any email.

**Syntax**  mail from <from>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;from&gt;</td>
<td>The email address that the mail is sent from.</td>
</tr>
</tbody>
</table>

**Mode**  Global Configuration

**Example**  To set the email address from which you are sending mail to “kaji@nerv.com”, use the command:

```
awplus(config)# mail from kaji@nerv.com
```

**Related Commands**
- delete mail
- mail
- mail smtpserver
- show mail
mail smtpserver

**Overview**
This command sets the IP address of the SMTP server that your device sends email to. You must specify a mail server with this command before you can send any email.

**Syntax**
mail smtpserver <ip-address>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>Internet Protocol (IP) Address for the mail server specified.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Example**
To specify a mail server at 192.168.0.1, use the command:

```
awplus# mail smtpserver 192.168.0.1
```

**Related Commands**
- debug mail
- delete mail
- mail
- mail from
- show mail
- show counter mail
show counter mail

**Overview**  This command displays the mail counters.

**Syntax**  `show counter mail`

**Mode**  User Exec and Privileged Exec

**Output**  Figure 51-1: Example output from the `show counter mail` command

<table>
<thead>
<tr>
<th>Mail Client (SMTP) counters</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mails Sent</td>
<td>Mails Sent</td>
<td>The number of emails sent successfully since the last device restart.</td>
</tr>
<tr>
<td></td>
<td>Mails Sent Fails</td>
<td>The number of emails the device failed to send since the last device restart.</td>
</tr>
</tbody>
</table>

Table 51-1: Parameters in the output of the `show counter mail` command

**Example**  To show the emails in the queue use the command:

```
awplus# show counter mail
```

**Related Commands**

- `debug mail`
- `delete mail`
- `mail`
- `mail from`
- `show mail`
**show mail**

**Overview**  
This command displays the emails in the queue.

**Syntax**  
`show mail`

**Mode**  
Privileged Exec

**Example**  
To display the emails in the queue use the command:

```
awplus# show mail
```

**Related Commands**
- `delete mail`
- `mail`
- `show counter mail`
**Overview**  This command applies the functionality of the no `debug mail` command.
Introduction

Overview
This chapter provides an alphabetical reference for commands used to configure Remote Monitoring (RMON).

For an introduction to RMON and an RMON configuration example, see the RMON Feature Overview and Configuration Guide.

RMON is disabled by default in AlliedWare Plus™. No RMON alarms or events are configured.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Command List
• “rmon alarm” on page 2234
• “rmon collection history” on page 2236
• “rmon collection stats” on page 2237
• “rmon event” on page 2238
• “show rmon alarm” on page 2239
• “show rmon event” on page 2240
• “show rmon history” on page 2242
• “show rmon statistics” on page 2244
rmon alarm

Overview
Use this command to configure an RMON alarm to monitor the value of an SNMP object, and to trigger specified events when the monitored object crosses specified thresholds.

To specify the action taken when the alarm is triggered, use the event index of an event defined by the rmon event command.

Use the no variant of this command to remove the alarm configuration.

NOTE: Only alarms for switch port interfaces, not for VLAN interfaces, can be configured.

Syntax
rmon alarm <alarm-index> <oid> interval <1-2147483647> {delta|absolute} rising-threshold <1-2147483647> event <rising-event-index> falling-threshold <1-2147483647> event <falling-event-index> alarmstartup {1|2|3} [owner <owner>]
no rmon alarm <alarm-index>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;alarm-index&gt;</td>
<td>&lt;1-65535&gt; Alarm entry index value.</td>
</tr>
<tr>
<td>&lt;oid&gt;</td>
<td>The variable SNMP MIB Object Identifier (OID) name to be monitored, in the format etherStatsEntry.field.&lt;stats-index&gt;. For example, etherStatsEntry.5.22 is the OID for the etherStatsPkts field in the etherStatsEntry table for the interface defined by the &lt;stats-index&gt; 22 in the rmon collection stats command.</td>
</tr>
<tr>
<td>interval&lt;1-2147483647&gt;</td>
<td>Polling interval in seconds.</td>
</tr>
<tr>
<td>delta</td>
<td>The RMON MIB alarmSampleType: the change in the monitored MIB object value between the beginning and end of the polling interval.</td>
</tr>
<tr>
<td>absolute</td>
<td>The RMON MIB alarmSampleType: the value of the monitored MIB object.</td>
</tr>
<tr>
<td>rising-threshold&lt;1-2147483647&gt;</td>
<td>Rising threshold value of the alarm entry in seconds.</td>
</tr>
<tr>
<td>&lt;rising-event-index&gt;</td>
<td>&lt;1-65535&gt; 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.</td>
</tr>
<tr>
<td>falling-threshold&lt;1-2147483647&gt;</td>
<td>Falling threshold value of the alarm entry in seconds.</td>
</tr>
<tr>
<td>&lt;falling-event-index&gt;</td>
<td>&lt;1-65535&gt; 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.</td>
</tr>
</tbody>
</table>
RMON COMMANDS
RMON ALARM

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarmstartup (1</td>
<td>2</td>
</tr>
<tr>
<td>owner &lt;owner&gt;</td>
<td>Arbitrary owner name to identify the alarm entry.</td>
</tr>
</tbody>
</table>

Default
By default, there are no alarms.

Mode
Global Configuration

Usage
RMON alarms have a rising and falling threshold. Once the alarm monitoring is operating, you cannot have a falling alarm unless there has been a rising alarm and vice versa.

However, when you start RMON alarm monitoring, an alarm must be generated without the other type of alarm having first been triggered. The alarmstartup parameter allows this. It is used to say whether RMON can generate a rising alarm (1), a falling alarm (2) or either alarm (3) as the first alarm.

Note that the SNMP MIB Object Identifier (OID) indicated in the command syntax with <oid> must be specified as a dotted decimal value with the form etherStatsEntry.field.<stats-index>.

Example
To configure an alarm to monitor the change per minute in the etherStatsPkt value for interface 22 (defined by stats-index 22 in the rmon collection stats command), to trigger event 2 (defined by the rmon event command) when it reaches the rising threshold 400, and to trigger event 3 when it reaches the falling threshold 200, and identify this alarm as belonging to Maria, use the commands:

```
awplus# configure terminal
awplus(config)# rmon alarm 229 etherStatsEntry.22.5 interval 60 delta rising-threshold 400 event 2 falling-threshold 200 event 3 alarmstartup 3 owner maria
```

Related Commands
rmon collection stats
rmon event
rmon collection history

Overview
Use this command to create a history statistics control group to store a specified number of snapshots (buckets) of the standard RMON statistics for the switch port, and to collect these statistics at specified intervals. If there is sufficient memory available, then the device will allocate memory for storing the set of buckets that comprise this history control.

Use the no variant of this command to remove the specified history control configuration.

NOTE: Only a history for switch port interfaces, not for VLAN interfaces, can be collected.

Syntax
rmon collection history <history-index> [buckets <1-65535>] [interval <1-3600>] [owner <owner>]
no rmon collection history <history-index>

Parameter | Description
--- | ---
<history-index> | <1-65535> A unique RMON history control entry index value.
buckets <1-65535> | Number of requested buckets to store snapshots. Default 50 buckets.
interval <1-3600> | Polling interval in seconds. Default 1800 second polling interval.
owner<owner> | Owner name to identify the entry.

Default
The default interval is 1800 seconds and the default buckets is 50 buckets.

Mode
Interface Configuration

Example
To create a history statistics control group to store 200 snapshots with an interval of 500 seconds, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# rmon collection history 200 buckets 500 interval 600 owner herbert
```

To disable the history statistics control group, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no rmon collection history 200
```
**rmon collection stats**

**Overview**
Use this command to enable the collection of RMON statistics on a switch port, and assign an index number by which to access these collected statistics.

Use the `no` variant of this command to stop collecting RMON statistics on this switch port.

**NOTE:** *Only statistics for switch port interfaces, not for VLAN interfaces, can be collected.*

**Syntax**
```
 rmon collection stats <collection-index> [owner <owner>]
 no rmon collection stats <collection-index>
```

**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 stop collecting RMON statistics, use the commands:
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no rmon collection stats 200
```
rmon event

**Overview**
Use this command to create an event definition for a log or a trap or both. The event index for this event can then be referred to by the `rmon alarm` command.

Use the `no` variant of this command to remove the event definition.

**NOTE:** Only the events for switch port interfaces, not for VLAN interfaces, can be collected.

**Syntax**
```
rmon event <event-index> [description <description>|owner <owner>| trap <trap>]
rmon event <event-index> [log [description <description>|owner <owner>|trap <trap>]]
rmon event <event-index> [log trap [description <description>|owner <owner>]]
no rmon event <event-index>
```

**Default**
No event is configured by default.

**Mode**
Global Configuration

**Example**
To create an event definition for a log with an index of 299, use this command:
```
awplus# configure terminal
awplus(config)# rmon event 299 log description cond3 owner alfred
```

To to remove the event definition, use the command:
```
awplus# configure terminal
awplus(config)# no rmon event 299
```

**Related Commands**
rmon alarm

**Parameter**
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;event-index&gt;</code></td>
</tr>
<tr>
<td>log</td>
</tr>
<tr>
<td>trap</td>
</tr>
<tr>
<td>log trap</td>
</tr>
<tr>
<td>description &lt;description&gt;</td>
</tr>
<tr>
<td>owner &lt;owner&gt;</td>
</tr>
</tbody>
</table>
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 52-1: Example output from the `show rmon event` command

```plaintext
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 52-2: Example output from the `show rmon history` command

```
awplus#sh rmon history
history index = 56
  data source ifindex = 4501
  buckets requested = 34
  buckets granted = 34
  Interval = 2000
  Owner Andrew

history index = 458
  data source ifindex = 5004
  buckets requested = 400
  buckets granted = 400
  Interval = 1500
  Owner trev
```

*NOTE*: The following etherStats counters are not currently available for Layer 3 interfaces:

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets
**Example**  
To display the parameters specified on all the currently defined RMON history collections, use the commands:

```
awplus# show rmon history
```

**Related Commands**  
`rmon collection history`
show rmon statistics

**Overview**  Use this command to display the current values of the statistics for all the RMON statistics collections currently defined on the device.

*NOTE:* Only statistics for switch port interfaces, not for VLAN interfaces, can be shown.

**Syntax**  show rmon statistics

**Mode**  User Exec and Privileged Exec

**Example**  To display the current values of the statistics for all the RMON statistics collections, use the commands:

```
awplus# show rmon statistics
```

**Output**  Figure 52-3: 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
RMON COMMANDS
SHOW RMON STATISTICS

**Related Commands**
rm MON collection stats
Introduction

Overview  This chapter provides an alphabetical reference for commands used to configure Triggers. For more information, see the Triggers Feature Overview and Configuration Guide.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.
**Trigger Commands**

**Command List**

- “active (trigger)” on page 2248
- “day” on page 2249
- “debug trigger” on page 2251
- “description (trigger)” on page 2252
- “repeat” on page 2253
- “script” on page 2254
- “show debugging trigger” on page 2256
- “show running-config trigger” on page 2257
- “show trigger” on page 2258
- “test” on page 2263
- “time (trigger)” on page 2264
- “trap” on page 2266
- “trigger” on page 2267
- “trigger activate” on page 2268
- “type atmf node” on page 2269
- “type cpu” on page 2272
- “type interface” on page 2273
- “type memory” on page 2274
- “type periodic” on page 2275
- “type ping-poll” on page 2276
- “type reboot” on page 2277
- “type stack disabled-master” on page 2278
- “type stack link” on page 2279
- “type stack master-fail” on page 2280
- “type stack member” on page 2281
- “type time” on page 2282
- “type usb” on page 2283
- “undebug trigger” on page 2284
active (trigger)

**Overview**  
This command enables a trigger. This allows the trigger to activate when its trigger conditions are met.

The `no` variant of this command disables a trigger. While in this state the trigger cannot activate when its trigger conditions are met.

**Syntax**
- `active`
- `no active`

**Mode**  
Trigger Configuration

**Usage**  
Configure a trigger first before you use this command to activate it.

For information about configuring a trigger, see the Triggers Feature Overview and Configuration Guide.

**Examples**  
To enable trigger 172, so that it can activate when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 172
awplus(config-trigger)# active
```

To disable trigger 182, preventing it from activating when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 182
awplus(config-trigger)# no active
```

**Related Commands**
- `show trigger`
- `trigger`
**Overview**  This command specifies the days or date that the can trigger activate on. You can specify either:

- A specific date
- A specific day of the week
- A list of days of the week
- every day

By default, the trigger can activate on any day.

**Syntax**

day every-day

day <1-31> <month> <2000-2035>

day <weekday>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>every-day</td>
<td>Sets the trigger so that it can activate on any day.</td>
</tr>
<tr>
<td>&lt;1-31&gt;</td>
<td>Day of the month the trigger is permitted to activate on.</td>
</tr>
<tr>
<td>&lt;month&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;2000-2035&gt;</td>
<td>Sets the year that the trigger is permitted to activate in.</td>
</tr>
<tr>
<td>&lt;weekday&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Mode**  Trigger Configuration

**Usage**  For example trigger configurations that use the day command, see “Restrict Internet Access” and “Turn off Power to Port LEDs” in the Triggers Feature Overview and Configuration Guide.

**Examples**  To permit trigger 55 to activate on the 1 Jun 2010, use the commands:

awplus# configure terminal
awplus(config)# trigger 55
awplus(config-trigger)# day 1 Jun 2010

To permit trigger 12 to activate on a Mondays, Wednesdays and Fridays, use the commands:

awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# day monday wednesday friday
TRIGGER COMMANDS

DAY

Related Commands

show trigger
trigger
debug trigger

**Overview**  This command enables trigger debugging. This generates detailed messages about how your device is processing the trigger commands and activating the triggers.

The **no** variant of this command disables trigger debugging.

**Syntax**

```
debug trigger
no debug trigger
```

**Mode**  Privilege Exec

**Examples**  To start trigger debugging, use the command:

```
awplus# debug trigger
```

To stop trigger debugging, use the command:

```
awplus# no trigger
```

**Related Commands**

- `show debugging trigger`
- `show trigger`
- `test`
- `trigger`
- `undebug trigger`
description (trigger)

**Overview**
This command adds an optional description to help you identify the trigger. This description is displayed in show command outputs and log messages.

The `no` variant of this command removes a trigger's description. The show command outputs and log messages stop displaying a description for this trigger.

**Syntax**
description `<description>`
no description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;description&gt;</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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>}
```

**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
```

**Parameter**  | **Description**
---|---
*yes*|forever: The trigger repeats indefinitely, or until disabled.
*no*|once: The trigger activates only once.
*<1-4294967294>*: The trigger repeats the specified number of times.

**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**
<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-5&gt;</code></td>
</tr>
<tr>
<td><code>&lt;filename&gt;</code></td>
</tr>
</tbody>
</table>

**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 53-1: 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**
display 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:

```plaintext
awplus# show running-config trigger
```

**Related Commands**  show trigger
### show trigger

**Overview**
This command displays configuration and diagnostic information about the triggers configured on the device. Specify the `show trigger` command without any options to display a summary of the configuration of all triggers.

**Syntax**
```
show trigger [<1-250>|counter|full]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;1-250&gt;</code></td>
<td>Displays detailed information about a specific trigger, identified by its trigger ID.</td>
</tr>
<tr>
<td><code>counter</code></td>
<td>Displays statistical information about all triggers.</td>
</tr>
<tr>
<td><code>full</code></td>
<td>Displays detailed information about all triggers.</td>
</tr>
</tbody>
</table>

**Mode**
Privileged Exec

**Example**
To get summary information about all triggers, use the following command:
```
awplus# show trigger
```

Table 53-1: Example output from the `show trigger` command

<table>
<thead>
<tr>
<th>TR#</th>
<th>Type &amp; Details</th>
<th>Name</th>
<th>Ac</th>
<th>Te</th>
<th>Tr</th>
<th>Repeat</th>
<th>#Scr</th>
<th>Days/Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>USB (in)</td>
<td>Y N Y Continuous 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>smtwtfs</td>
</tr>
<tr>
<td>002</td>
<td>USB (out)</td>
<td>Y N Y Continuous 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>smtwtfs</td>
</tr>
<tr>
<td>003</td>
<td>CPU (80% any)</td>
<td>Busy CPU</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Continuous</td>
<td>1</td>
<td>smtwtfs</td>
</tr>
<tr>
<td>005</td>
<td>Periodic (30 min)</td>
<td>Regular status check</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Continuous</td>
<td>1</td>
<td>-mwtf-</td>
</tr>
<tr>
<td>007</td>
<td>Memory (85% up)</td>
<td>High mem usage</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Continuous</td>
<td>1</td>
<td>smtwtfs</td>
</tr>
<tr>
<td>011</td>
<td>Time (00:01)</td>
<td>Weekend access</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Continuous</td>
<td>1</td>
<td>-------s</td>
</tr>
<tr>
<td>013</td>
<td>Reboot</td>
<td></td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Continuous</td>
<td>2</td>
<td>smtwtfs</td>
</tr>
<tr>
<td>017</td>
<td>Interface (vlan1 ...</td>
<td>Change config for...</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Once</td>
<td>1</td>
<td>2-apr-2008</td>
</tr>
<tr>
<td>019</td>
<td>Ping-poll (5 up)</td>
<td>Connection to svr1</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Continuous</td>
<td>1</td>
<td>smtwtfs</td>
</tr>
</tbody>
</table>

Table 53-2: Parameters in the output of the `show trigger` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TR#</td>
<td>Trigger identifier (ID).</td>
</tr>
<tr>
<td>Type &amp; Details</td>
<td>The trigger type, followed by the trigger details in brackets.</td>
</tr>
<tr>
<td>Name</td>
<td>Descriptive name of the trigger configured with the description (trigger) command.</td>
</tr>
</tbody>
</table>
### Show Trigger Command

**Table 53-2: Parameters in the output of the `show trigger` command (cont.)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ac</td>
<td>Whether the trigger is active (Y), or inactive (N).</td>
</tr>
<tr>
<td>Te</td>
<td>Whether the trigger is in test mode (Y) or not (N).</td>
</tr>
<tr>
<td>Tr</td>
<td>Whether or not the trigger is enabled to send SNMP traps. See the <code>trap</code> command.</td>
</tr>
<tr>
<td>Repeat</td>
<td>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 <code>show trigger &lt;1-250&gt;</code> command.</td>
</tr>
<tr>
<td>#Scr</td>
<td>Number of scripts associated with the trigger.</td>
</tr>
<tr>
<td>Days/Date</td>
<td>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.</td>
</tr>
</tbody>
</table>

To display detailed information about trigger 3, use the command:

**awplus# show trigger 3**

**Figure 53-2:** Example output from the `show trigger` command for a specific trigger

```plaintext
awplus# show trigger 3
Trigger Configuration Details
------------------------------------------------------------
Trigger ..................... 1
Description ................. display cpu usage when pass 80%
Type and details .......... CPU (80% up)
Days ....................... 26-nov-2007
After ..................... 00:00:00
Before .................... 23:59:59
Active .................... Yes
Test ...................... No
Trap ...................... Yes
Repeat .................... 123 (0)
Modified .................. Tue Dec 20 02:26:03 1977
Number of activations .... 0
Last activation ........... not activated
Number of scripts ....... 1
  1. shocpu scp
  2. <not configured>
  3. <not configured>
  4. <not configured>
  5. <not configured>
------------------------------------------------------------
```

To display detailed information about all triggers, use the command:

**awplus# show trigger full**
Table 53-3: Example output from the `show trigger full` command

```plaintext
awplus#show trigger full
Trigger Configuration Details
------------------------------------------------------------
  Trigger ..................... 1
  Description ................. <no description>
  Type and details ............ USB (in)
  Days ........................ smtwtfs
  After ........................ 00:00:00
  Before ........................ 23:59:59
  Active ...................... Yes
  Test ........................ No
  Trap ........................ Yes
  Repeat ........................ Continuous
  Modified .................... Fri Sep 3 14:45:56 2010
  Number of activations ...... 0
  Last activation ............. not activated
  Number of scripts ........... 0
    1. <not configured>
    2. <not configured>
    3. <not configured>
    4. <not configured>
    5. <not configured>

  Trigger ..................... 2
  Description ................. <no description>
  Type and details ............ USB (out)
  Days ........................ smtwtfs
  After ........................ 00:00:00
  Before ........................ 23:59:59
  Active ...................... Yes
  Test ........................ No
  Trap ........................ Yes
  Repeat ........................ Continuous
  Modified .................... Fri Sep 3 14:45:56 2010
  Number of activations ...... 0
  Last activation ............. not activated
  Number of scripts ........... 0
    1. <not configured>
    2. <not configured>
    3. <not configured>
    4. <not configured>
    5. <not configured>
```

Table 53-4: Parameters in the output of the `show trigger full` and `show trigger` commands for a specific trigger

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger</td>
<td>The ID of the trigger.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive name of the trigger.</td>
</tr>
<tr>
<td>Type and</td>
<td>The trigger type and its activation conditions.</td>
</tr>
<tr>
<td>details</td>
<td></td>
</tr>
</tbody>
</table>
Table 53-4: Parameters in the output of the `show trigger full` and `show trigger` commands for a specific trigger (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days</td>
<td>The days on which the trigger is permitted to activate.</td>
</tr>
<tr>
<td>Date</td>
<td>The date on which the trigger is permitted to activate. Only displayed if configured, in which case it replaces “Days”.</td>
</tr>
<tr>
<td>Active</td>
<td>Whether or not the trigger is permitted to activate.</td>
</tr>
<tr>
<td>Test</td>
<td>Whether or not the trigger is operating in diagnostic mode.</td>
</tr>
<tr>
<td>Trap</td>
<td>Whether or not the trigger is enabled to send SNMP traps.</td>
</tr>
<tr>
<td>Repeat</td>
<td>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.</td>
</tr>
<tr>
<td>Modified</td>
<td>The date and time of the last time that the trigger was modified.</td>
</tr>
<tr>
<td>Number of activations</td>
<td>Number of times the trigger has been activated since the last restart of the device.</td>
</tr>
<tr>
<td>Last activation</td>
<td>The date and time of the last time that the trigger was activated.</td>
</tr>
<tr>
<td>Number of scripts</td>
<td>How many scripts are associated with the trigger, followed by the names of the script files in the order in which they run.</td>
</tr>
</tbody>
</table>

To display counter information about all triggers use the command:

```
awplus# show trigger counter
```

Figure 53-3: Example output from the `show trigger counter` command

```
awplus#show trigger counter
Trigger Module Counters
---------------------------------------------------------------------
Trigger activations ......................... 0
Time triggers activated today .............. 0
Periodic triggers activated today .......... 0
Interface triggers activated today .......... 0
Resource triggers activated today .......... 0
Reboot triggers activated today ............ 0
Ping-poll triggers activated today .......... 0
Stack master fail triggers activated today .... 0
Stack member triggers activated today ....... 0
---------------------------------------------------------------------
```
Table 53-5: Parameters in the output of the `show trigger counter` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger activations</td>
<td>Number of times a trigger has been activated.</td>
</tr>
<tr>
<td>Time triggers activated today</td>
<td>Number of times a time trigger has been activated today.</td>
</tr>
<tr>
<td>Periodic triggers activated today</td>
<td>Number of times a periodic trigger has been activated today.</td>
</tr>
<tr>
<td>Interface triggers activated today</td>
<td>Number of times an interface trigger has been activated today.</td>
</tr>
<tr>
<td>Resource triggers activated today</td>
<td>Number of times a CPU or memory resource trigger has been activated today.</td>
</tr>
<tr>
<td>Ping-poll triggers activated today</td>
<td>Number of times a ping-poll trigger has been activated today.</td>
</tr>
</tbody>
</table>

Related Commands

trigger
**test**

**Overview**
This command puts the trigger into a diagnostic mode. In this mode the trigger may activate but when it does it will not run any of the trigger’s scripts. A log message will be generated to indicate when the trigger has been activated.

The **no** variant of this command takes the trigger out of diagnostic mode, restoring normal operation. When the trigger activates the scripts associated with the trigger will be run, as normal.

**Syntax**
```
test
no test
```

**Mode**
Trigger Configuration

**Usage**
Configure a trigger first before you use this command to diagnose it. For information about configuring a trigger, see the Triggers Feature Overview and Configuration Guide.

**Examples**
To put trigger 5 into diagnostic mode, where no scripts will be run when the trigger activates, use the commands:
```bash
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:
```bash
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no test
```

**Related Commands**
```
show trigger
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>]}
**Usage**

For example trigger configurations that use the `time (trigger)` command, see “Restrict Internet Access” and “Turn off Power to Port LEDs” in the Triggers Feature Overview and Configuration Guide.

**Examples**

To allow trigger 63 to activate between midnight and 10:30am, use the commands:

```bash
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:

```bash
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:

```bash
awplus# configure terminal
awplus(config)# trigger 65
awplus(config-trigger)# time after 10:30:00 before 20:15:00
```

**Related Commands**

show trigger

trigger
**Overview**  This command enables the specified trigger to send SNMP traps.  Use the **no** variant of this command to disable the sending of SNMP traps from the specified trigger.

**Syntax**
```
trap
no trap
```

**Default**  SNMP traps are enabled by default for all defined triggers.

**Mode**  Trigger Configuration

**Usage**  You must configure SNMP before using traps with triggers. For more information, see:

- the SNMP MIBs Overview, for information about which MIB objects are supported.
- the SNMP Feature Overview and Configuration Guide.

Since SNMP traps are enabled by default for all defined triggers, a common usage will be for the **no** variant of this command to disable SNMP traps from a specified trap if the trap is only periodic. Refer in particular to AT-TRIGGER-MIB in the SNMP MIBs Overview for further information about the relevant SNMP MIB.

**Examples**

To enable SNMP traps to be sent from trigger 5, use the commands:
```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# trap
```

To disable SNMP traps being sent from trigger 205, use the commands:
```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no trap
```

**Related Commands**
- trigger
- show trigger
**trigger**

**Overview**
This command is used to access the Trigger Configuration mode for the specified trigger. Once Trigger Configuration mode has been entered the trigger type information can be configured and the trigger scripts and other operational parameters can be specified. At a minimum the trigger type information must be specified before the trigger can become active.

The no variant of this command removes a specified trigger and all configuration associated with it.

**Syntax**
```
trigger <1-250>
no trigger <1-250>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-250&gt;</td>
<td>A trigger ID.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Examples**
To enter trigger configuration mode for trigger 12 use the command:
```
awplus# trigger 12
```

To completely remove all configuration associated with trigger 12, use the command:
```
awplus# no trigger 12
```

**Related Commands**
show trigger
trigger activate
trigger activate

**Overview**  This command is used to manually activate a specified trigger from the Privileged Exec mode, which has been configured with the `trigger` command from the Global Configuration mode.

**Syntax**  trigger activate <1-250>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-250&gt;</td>
<td>A trigger ID.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Usage**  This command manually activates a trigger without the normal trigger conditions being met.

The trigger is activated even if it is configured as inactive. The scripts associated with the trigger will be executed even if the trigger is in the diagnostic test mode.

Triggers activated manually do not have their repeat counts decremented or their 'last triggered' time updated, and do not result in updates to the '[type] triggers today' counters.

**Example**  To manually activate trigger 12 use the command:

```
awplus# trigger activate 12
```

**Related Commands**  
- `show trigger`
- `trigger`
type atmf node

**Overview**  
This command configures a trigger to be activated at an AMF node join event or leave event.

**Syntax**  
type atmf node {join|leave}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>join</td>
<td>AMF node join event.</td>
</tr>
<tr>
<td>leave</td>
<td>AMF node leave event.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
-----------------------
nodel, 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:

```

```

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:

```

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

```

---

`
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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-100&gt;</td>
<td>The percentage of CPU usage at which to trigger.</td>
</tr>
<tr>
<td>up</td>
<td>Activate when CPU usage exceeds the specified level.</td>
</tr>
<tr>
<td>down</td>
<td>Activate when CPU usage drops below the specified level.</td>
</tr>
<tr>
<td>any</td>
<td>Activate when CPU usage passes the specified level in either direction.</td>
</tr>
</tbody>
</table>

**Mode**  
Trigger Configuration

**Usage**  
For an example trigger configuration that uses the **type cpu** command, see “Capture Unusual CPU and RAM Activity” in the Triggers Feature Overview and Configuration Guide.

**Examples**  
To configure trigger 28 to be a CPU trigger that activates when CPU usage exceeds 80% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 28
awplus(config-trigger)# type cpu 80 up
```

To configure trigger 5 to be a CPU trigger that activates when CPU usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65
```

or

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65 any
```

**Related Commands**  
show trigger
  
trigger
**type interface**

**Overview**  This command configures a trigger to activate based on the link status of an interface. The trigger can be activated when the interface becomes operational by using the **up** option, or when the interface closes by using the **down** option. The trigger can also be configured to activate when either one of these events occurs by using the **any** option.

**Syntax**  `type interface <interface> [up|down|any]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interface&gt;</code></td>
<td>Interface name. This can be the name of a device port, an eth-management port, or a VLAN.</td>
</tr>
<tr>
<td><strong>up</strong></td>
<td>Activate when interface becomes operational.</td>
</tr>
<tr>
<td><strong>down</strong></td>
<td>Activate when the interface closes.</td>
</tr>
<tr>
<td><strong>any</strong></td>
<td>Activate when any interface link status event occurs.</td>
</tr>
</tbody>
</table>

**Mode**  Trigger Configuration

**Example**  To configure trigger 19 to be an interface trigger that activates when `port1.0.2` becomes operational, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 19
awplus(config-trigger)# type interface port1.0.2 up
```

**Related Commands**  `show trigger`

 trigger
**TRIGGER COMMANDS**

**TYPE MEMORY**

---

**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]

**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
```

or

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65 any
```

**Related Commands**

show trigger
toggle

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-100&gt;</td>
<td>The percentage of memory usage at which to trigger.</td>
</tr>
<tr>
<td>up</td>
<td>Activate when memory usage exceeds the specified level.</td>
</tr>
<tr>
<td>down</td>
<td>Activate when memory usage drops below the specified level.</td>
</tr>
<tr>
<td>any</td>
<td>Activate when memory usage passes the specified level in either direction.</td>
</tr>
</tbody>
</table>
**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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-1440&gt;</td>
<td>The number of minutes between activations.</td>
</tr>
</tbody>
</table>

**Mode**  Trigger Configuration

**Usage**  A combined limit of 10 triggers of the type periodic and time can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or periodic
```

For an example trigger configuration that uses the `type periodic` command, see “See Daily Statistics” in the Triggers Feature Overview and Configuration Guide.

**Example**  To configure trigger 44 to activate periodically at 10 minute intervals use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 44
awplus(config-trigger)# type periodic 10
```

**Related Commands**  
- `show trigger`
- `trigger`
**type ping-poll**

**Overview**  
This command configures a trigger that activates when Ping Polling identifies that a target device's status has changed. This allows you to run a configuration script when a device becomes reachable or unreachable.

**Syntax**  
type ping-poll <1-100> {up|down}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-100&gt;</td>
<td>The ping poll ID.</td>
</tr>
<tr>
<td>up</td>
<td>The trigger activates when ping polling detects that the target is reachable.</td>
</tr>
<tr>
<td>down</td>
<td>The trigger activates when ping polling detects that the target is unreachable.</td>
</tr>
</tbody>
</table>

**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 stack disabled-master

**Overview**  This command (configured to the stack) configures a trigger to activate on a stack member if it becomes the disabled master.

A disabled master has the same configuration as the active master, but has all its links shutdown.

Although this command could activate any trigger script, the intention here is that the script will reactivate the links from their previously shutdown state, to enable the user to manage the device. An appropriate trigger script must already exist that will apply the `shutdown` command on the deactivated links.

**CAUTION:** It is important that any ports that are configured as trunked ports across master and stack members are disabled at their stack member termination when operating in the fallback configuration. Otherwise, the trunked ports will not function correctly on the device that is connected downstream.

If the `stack virtual-mac` command command is enabled, the stack uses a virtual MAC address. The stack will always use this MAC address and the new elected master will still retain the originally configured virtual MAC address. If the `stack virtual-mac` command is disabled, the stack will use the MAC address of the current master. If the stack master fails, the stack MAC address changes to reflect the new master’s MAC address. For more information about virtual MAC addresses, see the VCStack Feature Overview and Configuration Guide.

**Syntax**  
type stack disabled-master

**Mode**  Trigger Configuration

**Examples**  To configure trigger 82 to activate on a device if it becomes the disabled master, use the commands. These commands enter the Trigger Configuration mode for trigger 82, specify the trigger type, and then specify the script to run.

```
awplus# configure terminal
awplus(config)# trigger 82
awplus(config-trigger)# type stack disabled master
awplus(config-trigger)# script 1 flash:/disabled.scp
awplus(config-trigger)# exit
```

**Related Commands**  
stack disabled-master-monitoring
trigger
type stack disabled-master
type stack member
type stack link
**type stack link**

**Overview**  
This command (configured to the stack) initiates the action of a pre-configured trigger to occur when a stacking link is either activated or deactivated.

**Syntax**  
`type stack link {up|down}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>up</td>
<td>Stack link up event</td>
</tr>
<tr>
<td>down</td>
<td>Stack link down event</td>
</tr>
</tbody>
</table>

**Mode**  
Trigger Configuration

**Example**  
To configure trigger 86 to activate when the stack link down event occurs, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type stack link down
```

**Related Commands**  
- `show trigger`
- `trigger`
- `type stack master-fail`
**type stack master-fail**

**Overview**  This command (configured to the stack) initiates the action of a pre-configured trigger to occur when the stack enters the fail-over state.

**Syntax**  
```bash
type stack master-fail
```

**Mode**  Trigger Configuration

**Example**  To configure trigger 86 to activate when stack master fail-over event occurs, use the commands:

```bash
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type stack master-fail
```

**Related Commands**
- `stack disabled-master-monitoring`
- `trigger`
- `type stack disabled-master`
- `type stack member`
- `type stack link`
**type stack member**

**Overview**  This command (configured to the stack) initiates the action of a pre-configured trigger to occur when a device either joins or leaves the stack.

**Syntax**  
```
type stack member {join|leave}
```

**Parameter** | **Description**
---|---
join | Neighbor join event
leave | Neighbor leave event

**Mode**  Trigger Configuration

**Example**  To configure a pre-configured trigger number 86 to activate when a new device joins the stack.

Note that the number 86 has no particular significance: you can assign any (previously created) numbered trigger.

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type stack member join
```

**Related Commands**  
- trigger
- type stack master-fail
- type stack link
type time

Overview  This command configures a trigger that activates at a specified time of day.

Syntax  type time <hh:mm>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="">hh:mm</a></td>
<td>The time to activate the trigger.</td>
</tr>
</tbody>
</table>

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}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>Trigger activates on insertion of a USB storage device.</td>
</tr>
<tr>
<td>out</td>
<td>Trigger activates on removal of a USB storage device.</td>
</tr>
</tbody>
</table>

**Mode**  Trigger Configuration

**Usage**  USB triggers cannot execute script files from a USB storage device.

For example trigger configurations that use the `type usb` command, see “Capture Show Output and Save to a USB Storage Device” in the Triggers Feature Overview and Configuration Guide.

**Examples**  To configure trigger 1 to activate on the insertion of a USB storage device, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 1
awplus(config-trigger)# type usb in
```

**Related Commands**

- trigger
- show running-config trigger
- show trigger
**Overview**  This command applies the functionality of the no debug trigger command.
Introduction

This chapter provides an alphabetical reference for commands used to configure Ping Polling. For more information, see the Ping Polling Feature Overview and Configuration Guide.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

Table 54-1: The following table lists the default values when configuring a ping poll

<table>
<thead>
<tr>
<th>Default</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical-interval</td>
<td>1 second</td>
</tr>
<tr>
<td>Description</td>
<td>No description</td>
</tr>
<tr>
<td>Fail-count</td>
<td>5</td>
</tr>
<tr>
<td>Length</td>
<td>32 bytes</td>
</tr>
<tr>
<td>Normal-interval</td>
<td>30 seconds</td>
</tr>
<tr>
<td>Sample-size</td>
<td>5</td>
</tr>
<tr>
<td>Source-ip</td>
<td>The IP address of the interface from which the ping packets are transmitted</td>
</tr>
<tr>
<td>Time-out</td>
<td>1 second</td>
</tr>
<tr>
<td>Up-count</td>
<td>30</td>
</tr>
</tbody>
</table>
**Command List**

- “active (ping-polling)” on page 2286
- “clear ping-poll” on page 2287
- “critical-interval” on page 2288
- “debug ping-poll” on page 2289
- “description (ping-polling)” on page 2290
- “fail-count” on page 2291
- “ip (ping-polling)” on page 2292
- “length (ping-poll data)” on page 2293
- “normal-interval” on page 2294
- “ping-poll” on page 2295
- “sample-size” on page 2296
- “show counter ping-poll” on page 2298
- “show ping-poll” on page 2300
- “source-ip” on page 2304
- “timeout (ping polling)” on page 2305
- “up-count” on page 2306
- “undebug ping-poll” on page 2307
## 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}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-100&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>all</td>
<td>Clears the counters and changes the device status of all polling instances.</td>
</tr>
</tbody>
</table>

**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

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65536&gt;</td>
<td>Time in seconds between pings, when the device has failed to a ping, or the device is unreachable.</td>
</tr>
</tbody>
</table>
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}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-100&gt;</td>
<td>A unique ping poll ID number.</td>
</tr>
<tr>
<td>all</td>
<td>Turn off all ping-poll debugging.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;description&gt;</code></td>
<td>The description of the target. Valid characters are any printable character and spaces. There is no maximum character length.</td>
</tr>
</tbody>
</table>

**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**  
```plaintext
fail-count <1-100>
no fail-count
```

**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:

```plaintext
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:

```plaintext
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-100&gt;</td>
<td>The number of pings within the sample size that a reachable device must fail to respond to before it is classified as unreachable.</td>
</tr>
</tbody>
</table>
**Overview**
This command specifies the IPv4 address of the device you are polling.

**Syntax**
```
ip {<ip-address>|<ipv6-address>}
```

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>An IPv4 address in dotted decimal notation A.B.C.D</td>
</tr>
<tr>
<td><code>&lt;ipv6-address&gt;</code></td>
<td>An IPv6 address in hexadecimal notation X:X::X:X</td>
</tr>
</tbody>
</table>
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
```

**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

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;4-1500&gt;</td>
<td>The number of data bytes to include in the data portion of the ping packet.</td>
</tr>
</tbody>
</table>
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
```

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-65536&gt;</td>
<td>Time in seconds between pings when the target is reachable.</td>
</tr>
</tbody>
</table>
**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>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-100&gt;</td>
<td>A unique ping poll ID number.</td>
</tr>
</tbody>
</table>

**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`
PING-POLLING COMMANDS
SAMPLE-SIZE

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-100&gt;</td>
<td>Number of pings that determines critical and up counts.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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:

```plaintext
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
--- | ---
<i-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 54-1: 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
```
PING-POLLING COMMANDS
SHOW COUNTER PING-POLL

Table 54-2: Parameters in output of the **show counter ping-poll** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping-poll</td>
<td>The ID number of the polling instance.</td>
</tr>
<tr>
<td>PingsSent</td>
<td>The total number of pings generated by the polling instance.</td>
</tr>
<tr>
<td>PingsFailedUpState</td>
<td>The number of unanswered pings while the target device is in the Up state.</td>
</tr>
<tr>
<td></td>
<td>This is a cumulative counter for multiple occurrences of the Up state.</td>
</tr>
<tr>
<td>PingsFailedDownState</td>
<td>Number of unanswered pings while the target device is in the Down state.</td>
</tr>
<tr>
<td></td>
<td>This is a cumulative counter for multiple occurrences of the Down state.</td>
</tr>
<tr>
<td>ErrorSendingPing</td>
<td>The number of pings that were not successfully sent to the target device.</td>
</tr>
<tr>
<td></td>
<td>This error can occur when your device does not have a route to the destination.</td>
</tr>
<tr>
<td>CurrentUpCount</td>
<td>The current number of sequential ping replies.</td>
</tr>
<tr>
<td>CurrentFailCount</td>
<td>The number of ping requests that have not received a ping reply in the current sample-size window.</td>
</tr>
<tr>
<td>UpStateEntered</td>
<td>Number of times the target device has entered the Up state.</td>
</tr>
<tr>
<td>DownStateEntered</td>
<td>Number of times the target device has entered the Down state.</td>
</tr>
</tbody>
</table>

**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**
--- | ---
<i-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 54-2:  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 54-3: Parameters in output of the `show ping-poll brief` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>The ID number of the polling instance, set when creating the polling instance with the <code>ping-poll</code> command.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether the polling instance is enabled or disabled.</td>
</tr>
</tbody>
</table>
PING-POLLING COMMANDS

SHOW PING-POLL

Table 54-3: Parameters in output of the **show ping-poll brief** command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>The current status of the device being polled:</td>
</tr>
<tr>
<td></td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>Down</td>
</tr>
<tr>
<td>Critical</td>
<td>Up</td>
</tr>
<tr>
<td>Critical</td>
<td>Down</td>
</tr>
<tr>
<td>Destination</td>
<td>The IP address of the polled device, set with the <strong>ip (ping-polling)</strong> command.</td>
</tr>
</tbody>
</table>

Figure 54-3: 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 54-4: Parameters in output of the **show ping-poll** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Optional description set for the polling instance with the <strong>description (ping-polling)</strong> command.</td>
</tr>
<tr>
<td>Destination IP address</td>
<td>The IP address of the polled device, set with the <strong>ip (ping-polling)</strong> command.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the device being polled:</td>
</tr>
<tr>
<td>Up</td>
<td>The device is reachable.</td>
</tr>
<tr>
<td>Down</td>
<td>The device is unreachable.</td>
</tr>
<tr>
<td>Critical Up</td>
<td>The device is reachable but recently the polling instance has not received some ping replies, so the polled device may be going down.</td>
</tr>
<tr>
<td>Critical Down</td>
<td>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.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether the polling instance is enabled or disabled. The <strong>active (ping-polling)</strong> and <strong>active (ping-polling)</strong> commands enable and disable a polling instance.</td>
</tr>
<tr>
<td>Source IP address</td>
<td>The source IP address sent in the ping packets. This is set using the <strong>source-ip</strong> command.</td>
</tr>
<tr>
<td>Critical interval</td>
<td>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 <strong>critical-interval</strong> command.</td>
</tr>
<tr>
<td>Normal interval</td>
<td>The time period between pings when the device is reachable. This is set with the <strong>normal-interval</strong> command.</td>
</tr>
<tr>
<td>Fail count</td>
<td>The number of pings that must be unanswered, within the total number of pings specified by the <strong>sample-size</strong> command, for the polling instance to consider the device unreachable. This is set using the <strong>fail-count</strong> command.</td>
</tr>
<tr>
<td>Up count</td>
<td>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 <strong>up-count</strong> command.</td>
</tr>
<tr>
<td>Sample size</td>
<td>The total number of pings that the polling instance inspects when determining whether a device is unreachable. This is set using the <strong>sample-size</strong> command.</td>
</tr>
<tr>
<td>Length</td>
<td>The number of data bytes to include in the data portion of the ping packet. This is set using the <strong>length (ping-poll data)</strong> command.</td>
</tr>
</tbody>
</table>
PING-POLLING COMMANDS

SHOW PING-POLL

Table 54-4: Parameters in output of the show ping-poll command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>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.</td>
</tr>
<tr>
<td>Debugging</td>
<td>Indicates whether ping polling debugging is Enabled or Disabled. This is set using the debug ping-poll command.</td>
</tr>
</tbody>
</table>

Examples

To display the ping poll settings and the status of all the polls, use the command:

```
awplus# show ping-poll
```

To display a summary of the ping poll settings, use the command:

```
awplus# show ping-poll brief
```

To display the settings for ping poll 6, use the command:

```
awplus# show ping-poll 6
```

To display a summary of the state of ping poll 6, use the command:

```
awplus# show ping-poll 6 brief
```

To display the settings of ping polls that have reachable devices, use the command:

```
awplus# show ping-poll state up
```

To display a summary of ping polls that have unreachable devices, use the command:

```
awplus# show ping-poll 6 state down brief
```

Related Commands

```
debug ping-poll
ping-poll
```
source-ip

**Overview**  This command specifies the source IP address to use in ping packets. By default, the polling instance uses the address of the interface through which it transmits the ping packets. It uses the device’s local interface IP address when it is set. Otherwise, the IP address of the interface through which it transmits the ping packets is used. The **no** variant of this command resets the source IP in the packets to the device’s local interface IP address.

**Syntax**

```
source-ip {<ip-address>|<ipv6-address>}
no source-ip
```

**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**  
```plaintext
timeout <1-30>
no timeout
```

**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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1-30&gt;</td>
<td>Length of time, in seconds, that the polling instance waits for a response from the polled device.</td>
</tr>
</tbody>
</table>
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

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:

```bash
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:

```bash
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)
**Overview**  This command applies the functionality of the no `debug ping-poll` command.
55  sFlow Commands

Introduction

Overview  This chapter provides an alphabetical reference for sFlow commands.

Command List  •  “debug sflow” on page 2308
•  “debug sflow agent” on page 2309
•  “sflow agent (address)” on page 2310
•  “sflow collector (address)” on page 2312
•  “sflow collector max-datagram-size” on page 2314
•  “sflow enable” on page 2315
•  “sflow max-header-size” on page 2316
•  “sflow polling-interval” on page 2318
•  “sflow sampling-rate” on page 2319
•  “show debugging sflow” on page 2320
•  “show running-config sflow” on page 2322
•  “show sflow” on page 2323
•  “show sflow interface” on page 2325
•  “undebug sflow” on page 2326
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]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Interface information.</td>
</tr>
<tr>
<td>&lt;port-list&gt;</td>
<td>The ports for which sFlow debug is to be enabled. The ports to display information about. The port list can be:</td>
</tr>
<tr>
<td></td>
<td>• a switch port (e.g. port1.0.12)</td>
</tr>
<tr>
<td></td>
<td>• a continuous range of ports separated by a hyphen, e.g.</td>
</tr>
<tr>
<td></td>
<td>port1.0.1-1.0.24</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of ports and port ranges, e.g.</td>
</tr>
<tr>
<td></td>
<td>port1.0.1, port1.0.1-1.0.24</td>
</tr>
<tr>
<td>sampling</td>
<td>Debug sFlow sampling for the specified port(s).</td>
</tr>
<tr>
<td>polling</td>
<td>Debug sFlow polling for the specified port(s).</td>
</tr>
</tbody>
</table>

**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 (address)

**Overview**  This command sets the sFlow® agent IP address on the switch. This address is inserted into every sFlow datagram sent from the sFlow agent switch to the sFlow collector device. The sFlow collector can then use this address to uniquely identify and to access the switch, such as for SNMP. We therefore recommend that you change this address as little as possible.

Although the agent address can be set to any valid IPv4 or IPv6 address; we recommended that you set the sFlow® agent IP address to be the local address that is configured on the switch. For information on local addresses and how to set them up, see the interface (to configure) command. This ensures that the sFlow collector can maintain connectivity to the switch irrespective of the addition or deletion of 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}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>The IPv4 address of the switch that is acting as the sFlow agent.</td>
</tr>
<tr>
<td>&lt;ipv6-address&gt;</td>
<td>The IPv6 address of the switch that is acting as the sFlow agent. The IPv6 address uses the format XX::XX.</td>
</tr>
</tbody>
</table>

**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
```
SFLOW COMMANDS
SFLOW AGENT (ADDRESS)

**Related Commands**

- `show running-config sflow`
- `show sflow`
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]
}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>IPv4 address of the remote sFlow collector.</td>
</tr>
<tr>
<td>&lt;ipv6-address&gt;</td>
<td>IPv6 address of remote sFlow collector. The IPv6 address uses the format X:X::X:X.</td>
</tr>
<tr>
<td>port</td>
<td>Destination UDP port for sFlow datagrams sent to the collector.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>UDP port number (default: 6343).</td>
</tr>
</tbody>
</table>

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 192.0.2.25 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
```
SFLOW COMMANDS
SFLOW COLLECTOR (ADDRESS)

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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;200-1500&gt;</td>
<td>The maximum number of bytes that can be sent in an sFlow datagram sent from the agent to the collector.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;14-200&gt;</td>
<td>The maximum number of header bytes to be sampled.</td>
</tr>
</tbody>
</table>

**Default**  The max-header-size is 128 bytes.

**Mode**  Interface Configuration

**Usage**  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
```

**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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disable polling (the default).</td>
</tr>
<tr>
<td>&lt;1-16777215&gt;</td>
<td>The polling interval in seconds.</td>
</tr>
</tbody>
</table>
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 {0|<256-16777215>}
no sflow sampling-rate
```

**Parameter** | **Description**
--- | ---
0 | Sets the default.
<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 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 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>]
```

**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**
```
awplus# show debugging sflow interface port1.0.1-1.0.9
sFlow Agent Debug: Enabled

<table>
<thead>
<tr>
<th>Port</th>
<th>Sampling Debug</th>
<th>Polling Debug</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.1</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>1.0.2</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>1.0.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.6</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>1.0.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.8</td>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td>1.0.9</td>
<td></td>
<td>Enabled</td>
</tr>
</tbody>
</table>
```
To display sFlow debug settings for all ports, use the command:
```
awplus# show debugging sflow
```
SFLOW COMMANDS
SHOW DEBUGGING SFLOW

Related Commands
- show running-config sfflow
- show sfflow 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 55-2: 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 55-1: Example output from the *show sflow* command

<table>
<thead>
<tr>
<th>sFlow Agent Configuration:</th>
<th>Default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>sFlow Admin Status .......... Disabled</td>
<td>[Disabled]</td>
</tr>
<tr>
<td>sFlow Agent Address .......... [not set]</td>
<td>[not set]</td>
</tr>
<tr>
<td>Collector Address .......... 0.0.0.0</td>
<td>[0.0.0.0]</td>
</tr>
<tr>
<td>Collector UDP Port ........ 6343</td>
<td>[6343]</td>
</tr>
<tr>
<td>Tx Max Datagram Size ...... 1200</td>
<td>[1400]</td>
</tr>
</tbody>
</table>

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 55-2: Parameters in the output of the *show sflow* command

<table>
<thead>
<tr>
<th>Output Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sFlow Admin Status</td>
<td>Whether sFlow agent operation is administratively enabled.</td>
</tr>
<tr>
<td>sFlow Agent Address</td>
<td>The sFlow agent IPv4 or IPv6 address for the device. sFlow is rendered inactive whenever the agent address is not set.</td>
</tr>
<tr>
<td>Collector Address</td>
<td>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.</td>
</tr>
<tr>
<td>Collector UDP Port</td>
<td>The UDP port on the collector to which sFlow datagrams are sent.</td>
</tr>
</tbody>
</table>
Table 55-2: Parameters in the output of the show sflow command (cont.)

<table>
<thead>
<tr>
<th>Output Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Max Datagram Size</td>
<td>The maximum size of the sFlow datagrams sent to the collector.</td>
</tr>
<tr>
<td>Polling/sampling/Tx</td>
<td>Whether sFlow sampling and/or polling (and hence sFlow datagram transmission) are active. If inactive the reasons are listed.</td>
</tr>
</tbody>
</table>

Related Commands
- show running-config sflow
- show sflow interface
show sflow interface

**Overview**  
This command displays sFlow agent sampling and polling configuration for specified ports.

**Syntax**  
show sflow interface 

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ifrange&gt;</td>
<td>The interface range.</td>
</tr>
</tbody>
</table>

**Mode**  
Privileged Exec
**Overview**  This command applies the functionality of the **no** variant of the `debug sflow` command.
Introduction

Overview This chapter provides an alphabetical reference of commands used to test copper cables. For more information on running the CFL, see the “Cable Fault Locator” Feature Overview and Configuration Guide.

Command List
- “clear test cable-diagnostics tdr” on page 2328
- “show test cable-diagnostics tdr” on page 2329
- “test cable-diagnostics tdr interface” on page 2330
**clear test cable-diagnostics tdr**

**Overview**  
This command clears 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
```
show test cable-diagnostics tdr

**Overview**  This command displays the results of the last cable-diagnostics test that was run using the TDR (Time Domain Reflectometry) 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 56-1:  Example output from the `show test cable-diagnostics tdr` command

<table>
<thead>
<tr>
<th>Port</th>
<th>Pair</th>
<th>Length</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.1</td>
<td>A</td>
<td>-</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>-</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>5 +/- 5 m</td>
<td>Open</td>
</tr>
</tbody>
</table>
**test cable-diagnostics tdr interface**

**Overview**  This command applies 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 “Cable Fault Locator” 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>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cable-diagnostics</td>
<td>The cable diagnostic tests.</td>
</tr>
<tr>
<td>tdr</td>
<td>Time Domain Reflectometry.</td>
</tr>
<tr>
<td>interface</td>
<td>Selects the interface to test.</td>
</tr>
<tr>
<td>&lt;interface&gt;</td>
<td>Interface number of the port to be tested, i.e. 1.0.2.</td>
</tr>
</tbody>
</table>

**Example**  To run a cable test on the cable inserted into port 1.0.1 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.
```
Introduction

Overview
This chapter provides an alphabetical reference for each of the Stacking commands.

Also note the following stacking trigger commands that are documented in the Triggers chapter:

type stack disabled-master command

type stack master-fail command

type stack member command

type stack link command

In addition to the stacking commands shown in this chapter, stacking content also exists in the following commands:

hostname command
reboot command
reload command
show cpu command
show cpu history command
show exception log command
show file systems command
show memory command
show memory history command
show process command
show system command

CAUTION: Stack operation is only supported if stack virtual-mac is enabled. For more information refer to stack virtual-mac on page 2367
STACKING COMMANDS

Command List • Command List
clear counter stack

**Overview**  This command clears all stack counters for all stack members.

**Syntax**  clear counter stack

**Mode**  Privileged Exec

**Example**  To clear all stack counters:

```
awplus# clear counter stack
```

**Related Commands**  show counter stack
### debug stack

**Overview**  
This command enables the stacking debugging facilities.

**Syntax**  
```plaintext
debug stack [link|topology|trace]
no debug stack [link|topology|trace]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>link</td>
<td>Stacking neighbor discovery events on stack links.</td>
</tr>
<tr>
<td>topology</td>
<td>Stacking topology discovery messages.</td>
</tr>
<tr>
<td>trace</td>
<td>Notable stacking events.</td>
</tr>
</tbody>
</table>

**Default**  
Stack trace debugging is enabled.

**Mode**  
Privileged Exec and Global Configuration

**Usage**  
The command displays debug information about the stacked devices. If no parameter is specified, all the stack debugging information will be displayed, including link events, topology discovery messages and all notable stacking events. If link parameter is specified, only the link events debugging information will be displayed.

**Examples**  
To enable debugging, enter the following command on the stack master:

```
awplus# debug stack
```

To enable link debugging, enter the following command on the stack master:

```
awplus# debug stack link
```

To enable topology discovery debugging, enter the following command on the stack master:

```
awplus# debug stack topology
```

To enable stack trace debugging, enter the following command on the stack master:

```
awplus# debug stack trace
```

**Related Commands**  
unddebug stack
reboot rolling

Overview
This command reboots a stack in a rolling sequence to minimize downtime.
The stack master is rebooted, causing the remaining stack members to failover and
elect a new master. The rebooted unit remains separate from the remaining stack
and boots up as a stand-alone unit. Once the rebooted unit has finished running
its configuration and has brought its ports up, it reboots all the remaining stack
members at once.

Syntax
reboot rolling

Mode
Privileged Exec

Usage
If you are upgrading to a new software version, the new version must also support
rolling reboot.

NOTE: When stacking is used with EPSR, the EPSR failovertime must be set to at least
5 seconds to avoid any broadcast storms during failover. Broadcast storms may occur
if the switch cannot failover quickly enough before the EPSR failovertime expires. For
further information about EPSR failovertime, see the epsr command.

Examples
To rolling reboot the stack, use the following commands:

awplus# reboot rolling
Continue the rolling reboot of the stack? (y/n):

After running this command, the stack master will reboot immediately with the
configuration file settings. The remaining stack members will then reboot once the
master has finished re-configuring.

Continue the rolling reboot of the stack? (y/n):

awplus# y

Related Commands
boot system
epsr
reload rolling

**Overview**  This command performs the same function as the `reboot rolling` command.
remote-command (deleted)

**Overview**  This command has been deleted. Instead, please use the remote-login command, and then run the command you need to run remotely.
remote-login

**Overview**  This command is used only on the master in order to log onto the CLI of another stack member. In most respects the result of this is similar to being logged into the stack master. Configuration commands are still applied to all stack members, but show commands, and commands that access the file system are executed locally. The specific output obtained will vary greatly depending on the show command chosen.

**Syntax**  `remote-login <stack-ID>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;stack-ID&gt;</code></td>
<td>Stack member number, from 1 to 8.</td>
</tr>
</tbody>
</table>

**Mode**  Privileged Exec

**Usage**  Note that some commands such as `ping` or `telnet` are not available when the remote-login is used.

**Example**  To log onto stack member 2, use the following command:

```
awplus# remote-login 2
```

To return to the command prompt on the master stack member, type `exit`. 
show counter stack

**Overview**  Use this command to display stack related counter information.

**Syntax**  show counter stack

**Default**  All counters are reset when the stack member is rebooted.

**Mode**  User Exec and Privileged Exec

**Usage**  This displays the stacking counter information for every stack member.

**Examples**  To display the stacking counter information about the whole stack, use the following command.

```
awplus# show counter stack
```

Table 57-1: Example output from the **show counter stack** command

<table>
<thead>
<tr>
<th>Virtual Chassis Stacking counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack member 1:</td>
</tr>
<tr>
<td>Topology Event counters</td>
</tr>
<tr>
<td>Units joined                      ...........1</td>
</tr>
<tr>
<td>Units left                        ...........0</td>
</tr>
<tr>
<td>Links up                          ...........1</td>
</tr>
<tr>
<td>Links down                        ...........0</td>
</tr>
<tr>
<td>ID conflict                        ...........0</td>
</tr>
<tr>
<td>Master conflict                   ...........0</td>
</tr>
<tr>
<td>Master failover                   ...........0</td>
</tr>
<tr>
<td>Master elected                    ...........1</td>
</tr>
<tr>
<td>Master discovered                 ...........0</td>
</tr>
<tr>
<td>SW autoupgrades                    ...........0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stack Port 1 Topology Event counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link up                              ...........3</td>
</tr>
<tr>
<td>Link down                            ...........2</td>
</tr>
<tr>
<td>Nbr re-init                          ...........0</td>
</tr>
<tr>
<td>Nbr incompatible                     ...........0</td>
</tr>
<tr>
<td>Nbr 2way comms                       ...........1</td>
</tr>
<tr>
<td>Nbr full comms                       ...........1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stack Port 2 Topology Event counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link up                              ...........0</td>
</tr>
<tr>
<td>Link down                            ...........0</td>
</tr>
<tr>
<td>Nbr re-init                          ...........0</td>
</tr>
<tr>
<td>Nbr incompatible                     ...........0</td>
</tr>
<tr>
<td>Nbr 2way comms                       ...........0</td>
</tr>
<tr>
<td>Nbr full comms                       ...........0</td>
</tr>
</tbody>
</table>
Table 57-1: Example output from the **show counter stack** command (cont.)

<table>
<thead>
<tr>
<th>Topology Message counters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Total</td>
<td>..........4</td>
</tr>
<tr>
<td>Tx Hellos</td>
<td>..........4</td>
</tr>
<tr>
<td>Tx Topo DB</td>
<td>..........0</td>
</tr>
<tr>
<td>Tx Topo update</td>
<td>..........0</td>
</tr>
<tr>
<td>Tx Link event</td>
<td>..........0</td>
</tr>
<tr>
<td>Tx Reinitialise</td>
<td>..........0</td>
</tr>
<tr>
<td>Tx Port 1</td>
<td>..........4</td>
</tr>
<tr>
<td>Tx Port 2</td>
<td>..........0</td>
</tr>
<tr>
<td>Tx 1-hop transport</td>
<td>..........4</td>
</tr>
<tr>
<td>Tx Layer-2 transport</td>
<td>..........0</td>
</tr>
<tr>
<td>Rx Total</td>
<td>..........1</td>
</tr>
<tr>
<td>Rx Hellos</td>
<td>..........1</td>
</tr>
<tr>
<td>Rx Topo DB</td>
<td>..........0</td>
</tr>
<tr>
<td>Rx Topo update</td>
<td>..........0</td>
</tr>
<tr>
<td>Rx Link event</td>
<td>..........0</td>
</tr>
<tr>
<td>Rx Reinitialise</td>
<td>..........0</td>
</tr>
<tr>
<td>Rx Port 1</td>
<td>..........1</td>
</tr>
<tr>
<td>Rx Port 2</td>
<td>..........0</td>
</tr>
<tr>
<td>Rx 1-hop transport</td>
<td>..........1</td>
</tr>
<tr>
<td>Rx Layer-2 transport</td>
<td>..........0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topology Error counters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version unsupported</td>
<td>..........0</td>
</tr>
<tr>
<td>Product unsupported</td>
<td>..........0</td>
</tr>
<tr>
<td>XEM unsupported</td>
<td>..........0</td>
</tr>
<tr>
<td>Too many units</td>
<td>..........0</td>
</tr>
<tr>
<td>Invalid messages</td>
<td>..........0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resiliency Link counters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Health status good</td>
<td>..........1</td>
</tr>
<tr>
<td>Health status bad</td>
<td>..........0</td>
</tr>
<tr>
<td>Tx</td>
<td>..........0</td>
</tr>
<tr>
<td>Tx Error</td>
<td>..........0</td>
</tr>
<tr>
<td>Rx</td>
<td>..........3600</td>
</tr>
<tr>
<td>Rx Error</td>
<td>..........0</td>
</tr>
</tbody>
</table>

Stack member 2:

```
-- Output repeated for other stack members - details not shown --
```

Table 57-2: Parameters in the output of the **show counter stack** command

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Topology Event Counters</strong></td>
<td></td>
</tr>
<tr>
<td>Units joined</td>
<td>Number of times that the stack acquires a member.</td>
</tr>
<tr>
<td>Units left</td>
<td>Number of times that the stack loses a member.</td>
</tr>
<tr>
<td>Links up</td>
<td>Number of times that a stack link is up in the stack.</td>
</tr>
<tr>
<td>Links down</td>
<td>Number of times that a stack link is down in the stack.</td>
</tr>
<tr>
<td>ID conflict</td>
<td>Number of times that stack-ID conflicts.</td>
</tr>
</tbody>
</table>
### Parameters in the output of the `show counter stack` command (cont.)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master conflict</td>
<td>Number of times that stack master conflict occurs.</td>
</tr>
<tr>
<td>Master failover</td>
<td>Number of times that stack master fails.</td>
</tr>
<tr>
<td>Master elected</td>
<td>Number of times that stack master is elected.</td>
</tr>
<tr>
<td>Master discovered</td>
<td>Number of times that stack master is discovered.</td>
</tr>
<tr>
<td>SW autoupgrades</td>
<td>Number of times that the software in the stack members are auto upgraded.</td>
</tr>
<tr>
<td>Stack port</td>
<td></td>
</tr>
<tr>
<td>Link up</td>
<td>Number of times that this unit's physical stack link has come up.</td>
</tr>
<tr>
<td>Link down</td>
<td>Number of times that this unit's physical stack link has come down.</td>
</tr>
<tr>
<td>Nbr re-init</td>
<td>Number of times that the neighbor is detected as having reinitialised.</td>
</tr>
<tr>
<td>Nbr incompatible</td>
<td>Number of times that the neighbor is detected as incompatible.</td>
</tr>
<tr>
<td>Nbr 2way comms</td>
<td>Number of times that the neighbor is in two way communication status.</td>
</tr>
<tr>
<td>Nbr full comms</td>
<td>Number of times that the neighbor is in full communication status.</td>
</tr>
<tr>
<td>Topology message counters</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>Total number of topology messages.</td>
</tr>
<tr>
<td>Hellos</td>
<td>Number of hello messages.</td>
</tr>
<tr>
<td>Topology DB</td>
<td>Number of topology database messages.</td>
</tr>
<tr>
<td>Topology update</td>
<td>Number of topology database update messages.</td>
</tr>
<tr>
<td>Link event</td>
<td>Number of link event messages.</td>
</tr>
<tr>
<td>Reinitialise</td>
<td>Number of reinitialise messages.</td>
</tr>
<tr>
<td>1-hop transport</td>
<td>Number of 1-hop transport messages.</td>
</tr>
<tr>
<td>Layer-2 transport</td>
<td>Number of layer 2 transport messages.</td>
</tr>
<tr>
<td>Link event</td>
<td>Number of link event messages.</td>
</tr>
</tbody>
</table>
#### Table 57-2: Parameters in the output of the `show counter stack` command (cont.)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reinitialise</td>
<td>Number of reinitialise messages.</td>
</tr>
<tr>
<td>1-hop transport</td>
<td>Number of 1-hop transport messages.</td>
</tr>
<tr>
<td>Layer-2 transport</td>
<td>Number of Layer 2 transport messages.</td>
</tr>
<tr>
<td>Topology error counters</td>
<td>Reasons why a neighboring unit could not join the stack.</td>
</tr>
<tr>
<td>Version unsupported</td>
<td>Number of stack software version unsupported errors.</td>
</tr>
<tr>
<td>Product unsupported</td>
<td>Number of product unsupported errors.</td>
</tr>
<tr>
<td>XEM unsupported</td>
<td>Number of XEM unsupported errors.</td>
</tr>
<tr>
<td>Too many units</td>
<td>Number of too many units errors.</td>
</tr>
<tr>
<td>Invalid messages</td>
<td>Number of invalid messages.</td>
</tr>
<tr>
<td>Health status good</td>
<td>The number of times that the resiliency link has successfully carried healthchecks following a failure at startup.</td>
</tr>
<tr>
<td>Health status bad</td>
<td>The number of times that the resiliency link healthcheck has timed out. A timeout occurs when a backup stack member detects a delay greater than two seconds between healthcheck messages received.</td>
</tr>
<tr>
<td>Rx</td>
<td>The total number of healthcheck messages that a stack member has received from the stack master.</td>
</tr>
<tr>
<td>Rx Error</td>
<td>The total number of invalid healthcheck messages that have been received from the master. This message is not applicable to the stack master.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show stack`
- `switch provision (stack)`
show debugging stack

**Overview**  This command shows which debugging modes are currently enabled for stacking.

**Syntax**  show debugging stack

**Mode**  User Exec and Privileged Exec

**Example**  To display the stack debugging mode status, use the command:

```
awplus# show debugging stack
```

Figure 57-1:  Example output from the show debugging stack command

```
Virtual Chassis Stacking debugging status:
  VCS link debugging is on
  VCS topology debugging is on
  VCS trace debugging is on
```

**Related Commands**  debug stack
show running-config stack

**Overview**  Use this command to display the running system information specific to the stack.

```bash
show running-config stack
```

**Mode**  Privileged Exec and Global Configuration

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

```bash
awplus# show running-config stack
```

**Output**  Figure 57-2: Example output from the show running-config stack command

```
awplus#show running-config stack
stack virtual-mac
stack virtual-chassis-id 1982
stack management vlan 4000
stack management subnet 192.168.254.0
stack enable
stack 2 priority 20
```

**Related Commands**  show running-config
show provisioning (stack)

**Overview**  Use this command to display the provisioning status of all installed or provisioned hardware. Provisioning is the preconfiguration necessary to accommodate future connection of hardware items such as a switch.

**Syntax**  `show provisioning`

**Mode**  User Exec and Privileged Exec

**Example**  To show provisioning, use the following command:

```
awplus# show provisioning
```

**Output**  Figure 57-3: Example output from the `show provisioning` command

```
Switch
provisioning summary information

<table>
<thead>
<tr>
<th>ID</th>
<th>Board class</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>x510-28</td>
<td>Hardware present</td>
</tr>
</tbody>
</table>
```

Table 57-3: Parameters in the output of the `show provisioning` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The unit bay-location of the hardware provision.</td>
</tr>
<tr>
<td>Board class</td>
<td>The hardware type.</td>
</tr>
<tr>
<td>Status</td>
<td>The provisioned state:</td>
</tr>
<tr>
<td></td>
<td>• Hardware Present means that the hardware is currently installed in the stack.</td>
</tr>
<tr>
<td></td>
<td>• Provisioned means that although the hardware is not currently installed, the stack is preconfigured ready to accept the hardware installation.</td>
</tr>
</tbody>
</table>
show stack

Overview  Use this command to display information about current stack members.

Syntax  show stack [detail]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Display detailed stacking information.</td>
</tr>
</tbody>
</table>

Default  Display summary information only.

Mode  User Exec and Privileged Exec

Usage  This command displays information about current stack members. If the **detail** parameter is specified, additional information will be displayed for each stack member. By default, only summary information is displayed.

Example  To display summary information about the stack, use the command:

```plaintext
awplus# show stack
```

Output  Figure 57-4: Example output from the **show stack** command

<table>
<thead>
<tr>
<th>ID</th>
<th>Pending ID</th>
<th>MAC address</th>
<th>Priority</th>
<th>Status</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>0000.cd28.07e1</td>
<td>128</td>
<td>Ready</td>
<td>Active Master</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>0015.77c2.4d44</td>
<td>128</td>
<td>Ready</td>
<td>Backup Member</td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>0015.77c9.7464</td>
<td>128</td>
<td>Syncing</td>
<td>Backup Member</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Provisioned</td>
</tr>
</tbody>
</table>

Operational Status  Normal operation

Stack MAC address  0000.cd28.07e1

Table 57-4: Parameters in the output from the **show stack** command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Stack-ID.</td>
</tr>
<tr>
<td>MAC address</td>
<td>Stack member MAC address.</td>
</tr>
</tbody>
</table>
STACKING COMMANDS
SHOW STACK

Table 57-4: Parameters in the output from the show stack command (cont.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Stack member master election priority (between 0 and 255). Note that the lowest number has the highest priority.</td>
</tr>
<tr>
<td>Role</td>
<td>Stack member’s role in the stack, this can be one of:</td>
</tr>
<tr>
<td></td>
<td>• Active Master</td>
</tr>
<tr>
<td></td>
<td>• Disabled Master — this is the temporary master when there is a communication break within the stack, but communication still exists across the resiliency link. In this state all switch ports within the stack are disabled by default, but a different configuration can be run by a “type stack disabled-master” trigger.</td>
</tr>
<tr>
<td></td>
<td>• Backup Member — a device other than the stack master.</td>
</tr>
<tr>
<td></td>
<td>• Provisioned — indicates that the stack position is provisionally configured, i.e. ready to accept a particular switch type into the stack.</td>
</tr>
</tbody>
</table>

Example To display the detailed stacking information about the stack’s overall status:

awplus# show stack detail
Figure 57-5: Example output from the `show stack detail` command

```
<table>
<thead>
<tr>
<th>Stack Status:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Status: Normal operation</td>
</tr>
<tr>
<td>Management VLAN ID: 4094</td>
</tr>
<tr>
<td>Management VLAN subnet address: 192.168.255.0</td>
</tr>
<tr>
<td>Virtual Chassis ID: 388 (0x184)</td>
</tr>
<tr>
<td>Virtual MAC address: 0000.cd37.0184</td>
</tr>
<tr>
<td>Mixed mode: Disabled</td>
</tr>
<tr>
<td>Disabled Master Monitoring: Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stack member 1:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID: 1</td>
</tr>
<tr>
<td>Pending ID: -</td>
</tr>
<tr>
<td>MAC address: 0000.cd28.070d</td>
</tr>
<tr>
<td>Last role change: Wed May 7 22:31:58 2013</td>
</tr>
<tr>
<td>Product type: x510-52GTX</td>
</tr>
<tr>
<td>Role: Active Master</td>
</tr>
<tr>
<td>Priority: 1</td>
</tr>
<tr>
<td>Host name: awplus</td>
</tr>
<tr>
<td>S/W version auto synchronizaion: On</td>
</tr>
<tr>
<td>Resiliency link status: Configured</td>
</tr>
<tr>
<td>Stack port 1.0.51 status: learned neighbor 2</td>
</tr>
<tr>
<td>Stack port 1.0.52 status: learned neighbor 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stack member 2:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID: 2</td>
</tr>
<tr>
<td>Pending ID: -</td>
</tr>
<tr>
<td>MAC address: 0000.cd29.716d</td>
</tr>
<tr>
<td>Last role change: Wed May 7 23:47:21 2013</td>
</tr>
<tr>
<td>Product type: x510-52GTX</td>
</tr>
<tr>
<td>Role: Backup Member</td>
</tr>
<tr>
<td>Status: Ready</td>
</tr>
<tr>
<td>Priority: 2</td>
</tr>
<tr>
<td>Host name: awplus-2</td>
</tr>
<tr>
<td>S/W version auto synchronizaion: On</td>
</tr>
<tr>
<td>Resiliency link status: Successful</td>
</tr>
<tr>
<td>Stack port 2.0.51 status: learned neighbor 3</td>
</tr>
<tr>
<td>Stack port 2.0.52 status: learned neighbor 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stack member 3:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID: 3</td>
</tr>
<tr>
<td>Pending ID: -</td>
</tr>
<tr>
<td>MAC address: 0015.77c2.4d9d</td>
</tr>
<tr>
<td>Last role change: Wed May 7 22:31:58 2013</td>
</tr>
<tr>
<td>Product type: x510-52GTX</td>
</tr>
<tr>
<td>Role: Backup Member</td>
</tr>
<tr>
<td>Priority: 3</td>
</tr>
<tr>
<td>Host name: awplus-3</td>
</tr>
<tr>
<td>S/W version auto synchronizaion: On</td>
</tr>
<tr>
<td>Resiliency link status: Successful</td>
</tr>
<tr>
<td>Stack port 3.0.51 status: learned neighbor 1</td>
</tr>
<tr>
<td>Stack port 3.0.52 status: learned neighbor 2</td>
</tr>
</tbody>
</table>
```
### Table 57-5: Parameters in the output from the `show stack detail` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S/W version auto synchronization</td>
<td>Whether the software-auto-synchronization feature is turned on or off.</td>
</tr>
<tr>
<td>Host name</td>
<td>The host name of the stack member.</td>
</tr>
<tr>
<td>ID</td>
<td>Stack-ID.</td>
</tr>
<tr>
<td>Last Role Change</td>
<td>The date and time the stack member last changed its role in the stack.</td>
</tr>
<tr>
<td>MAC address</td>
<td>Stack member MAC address.</td>
</tr>
<tr>
<td>Management VLAN ID</td>
<td>The VLAN ID currently used for stack management: the default is 4094.</td>
</tr>
<tr>
<td>Management VLAN subnet address</td>
<td>The current stacking management VLAN subnet address.</td>
</tr>
<tr>
<td>Virtual Chassis ID</td>
<td>The Virtual Chassis ID determines the last 12 bits of the Virtual MAC address: <code>0000.cd37.0xxx</code>.</td>
</tr>
<tr>
<td>Virtual MAC Address</td>
<td>The Virtual MAC address of the stack.</td>
</tr>
</tbody>
</table>
| Disabled Master Monitoring                    | The current Disabled Master Monitoring status. This can be:  
  - **Enabled**  
  - **Disabled**  
  - **Inactive**  
| Operational Status                            | The status of the stack. This can be:  
  - **Normal operation:**  
    If any other status is displayed, it may warrant further investigation.  
  - **Stacking hardware disabled:**  
    Use the `stack enable` command to activate the stacking feature.  
  - **Operating in failover mode:**  
    This stack member has become separated from the rest of the stack, or it failed to join the stack correctly.  
  - **Standalone unit:**  
    Stacking is enabled, but no other stack members are present.  
  - **Not all stack ports are up:**  
    One or more stacking ports may be down, or stacking discovery may not have detected the neighbor successfully.                                                                 |
| Stack Status                                  | The stack’s overall status. Note that a warning is issued if the stack is not connected in a standard ring topology.                                                                                 |
Table 57-5: Parameters in the output from the `show stack detail` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending ID</td>
<td>The pending stack member ID. This can be changed by the <code>stack renumber</code> command. If there is no pending ID, the “-” symbol will display.</td>
</tr>
<tr>
<td>Stack port status</td>
<td>The status of the stack port. This can be:</td>
</tr>
<tr>
<td></td>
<td>• Down</td>
</tr>
<tr>
<td></td>
<td>• Neighbor incompatible</td>
</tr>
<tr>
<td></td>
<td>• Discovering neighbor</td>
</tr>
<tr>
<td></td>
<td>• Learned neighbor</td>
</tr>
<tr>
<td>Priority</td>
<td>Stack member master election priority (between 1 and 255) Note that the lowest number has the highest priority.</td>
</tr>
<tr>
<td>Product Type</td>
<td>Stack member product type. For example, x510-28GPX.</td>
</tr>
<tr>
<td>Provisioned</td>
<td>Indicates that the stack position is provisionally configured, i.e. ready to accept a particular switch type into the stack.</td>
</tr>
<tr>
<td>Resiliency link status</td>
<td>The current status of the resiliency link. The status can be one of:</td>
</tr>
<tr>
<td></td>
<td>• Not configured (Master or Member).</td>
</tr>
<tr>
<td></td>
<td>• Configured (Master only).</td>
</tr>
<tr>
<td></td>
<td>• Successful: Successfully receiving healthchecks from the Active Master.</td>
</tr>
<tr>
<td></td>
<td>• Failed (Member only): Not receiving any healthchecks from the Active Master.</td>
</tr>
<tr>
<td></td>
<td>• Stopped: The resiliency link is configured, but is inactive. This may occur in a Disabled Master stack, for example if the Disabled Master Monitoring feature is not used.</td>
</tr>
</tbody>
</table>
Table 57-5: Parameters in the output from the show stack detail command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Stack member’s role in the stack, this can be one of:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active Master</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled Master</strong> — The temporary master when there is a communication break within the stack, but communication still exists across the resiliency link. In this state all switch ports within the stack are disabled by default, but a different configuration can be run by a “<strong>type stack disabled-master</strong>” trigger command.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Backup Member</strong> — a device other than the stack master.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Discovering</strong> — joining the stack.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates how readily a stack member can take over as master if the current stack master were to fail.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Init</strong> — the stack member is completing the startup initialization.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Syncing</strong> — the stack member is synchronizing state information with the stack master following startup.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ready</strong> — the stack member is fully synchronized with the current master and is ready to take over immediately.</td>
</tr>
</tbody>
</table>

**Related Commands**
- show counter stack
- show stack resiliencylink
- stack disabled-master-monitoring
- stack resiliencylink
- stack software-auto-synchronize
### show stack resiliencylink

**Overview**  
Use this command to display information about the current status of the resiliency-link across the members of the stack.

**Syntax**  
`show stack resiliencylink`

**Mode**  
User Exec and Privileged Exec

**Example**  
To display information about the current status of the resiliency-link across the stack members, use the command:

```
awplus# show stack resiliencylink
```

**Output**  
Figure 57-6: Example output from the `show stack resiliencylink` command

```
awplus(config)# show stack resiliencylink
Stack member 1:
-----------------------------------------------------------
Status                         Configured
Interface                      vlan4093
Interface state                UP
Resiliency-link port(s)        port1.2.11

Stack member 2:
-----------------------------------------------------------
Status                         Successful
Interface                      vlan4093
Interface state                UP
Resiliency-link port(s)        port2.2.11
```

Table 57-6: Parameters in the output of the `show stack resiliencylink` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The current status of the stack member's resiliency link. Can be one of:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not configured</strong> (Master or Member).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Configured</strong> (Master only).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Successful</strong>: Successfully receiving healthchecks from the Active Master.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Failed</strong> (Member only): Not receiving any healthchecks from the Active Master.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Stopped</strong>: The resiliency link is configured, but is inactive. This may occur in a Disabled Master stack, for example if the Disabled Master Monitoring feature is not used.</td>
</tr>
<tr>
<td>Interface</td>
<td>The name of the VLAN interface that is connected to the resiliency link.</td>
</tr>
</tbody>
</table>
STACKING COMMANDS
SHOW STACK RESILIENCY LINK

Table 57-6: Parameters in the output of the `show stack resiliencylink` command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface state</td>
<td>The current status of the interface. Can be either up or down.</td>
</tr>
<tr>
<td>Resiliency-link port(s)</td>
<td>The switch port(s) the resiliency link is connected to.</td>
</tr>
</tbody>
</table>

Related Commands

- `switch provision (stack)`
- `show stack`
- `stack resiliencylink`
- `switchport resiliencylink`
stack disabled-master-monitoring

**Overview**
This command enables the Disabled Master Monitoring (DMM) feature. If a stack member becomes a disabled master, the DMM feature will use the stack resiliency link to continue monitoring the health of the separated stack master.

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

**Syntax**
```
stack disabled-master-monitoring
no stack disabled-master-monitoring
```

**Default**
By default, Disabled Master Monitoring is enabled. However, it only operates if there is a resiliency link.

**Mode**
Global Configuration

**Usage**
This command enables additional stack resiliency link functionality, which is used if a stack separation occurs. For DMM to operate, a resiliency link must also be configured (stack resiliencylink command). A stack separation could result in a stack member becoming a disabled master, which has the configuration as a normal stack master except that all its switchports are shutdown.

For more information about the disabled master state, see the VCStack Feature Overview and Configuration Guide.

When the DMM feature is enabled, the disabled master will continue to monitor the health of the original stack master over the stack resiliency link connection. If the original stack master were to fail, when the DMM feature is enabled, then the disabled master will detect this and will automatically re-enable its switchports. This ensures that the stack will continue to pass network traffic, even if a catastrophic stack failure occurs.

For more information about the DMM feature when the stack member is a disabled master, see the VCStack Feature Overview and Configuration Guide.

**Examples**
To enable the DMM feature, use the following commands:
```
awplus# configure terminal
awplus(config)# stack disabled-master-monitoring
```

To disable the DMM feature, use the following commands:
```
awplus# configure terminal
awplus(config)# no stack disabled-master-monitoring
```

**Related Commands**
- `switch provision (stack)`
- `show stack`
- `stack resiliencylink`
- `type stack disabled-master`
- `type stack master-fail`
stack enable

**Overview**  This command is used on a stackable stand-alone switch to manually turn on the VCStack feature.

This command can also be run on a switch that has previously been removed from a stack (by using the `no` variant of this command) and return it to stacking operation.

The `no` variant of this command removes a selected stack member switch, as specified by the `<stack-ID>` selection in the command syntax, from the virtual chassis stack.

**Syntax**

Stack enable  

```plaintext
stack enable

no stack <stack-ID> enable
```

**Parameter**  

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;stack-ID&gt;</code></td>
<td>Stack member number, from 1 to 8.</td>
</tr>
</tbody>
</table>

**Default**  
The VCStack feature is enabled by default. The feature automatically starts when hardware is present.

**Mode**  
Global Configuration

**Usage**  
When stack enable is entered, the stack virtual-mac is automatically enabled. Using virtual-mac is required in order to minimize disruption on failover.

Running the `no` variant of this command will remove the selected stack member from the stack. At this point the removed member will act as a stand-alone master and will disable all of its ports. The switch can then only be accessed via its console port. If the command is run on the master then all current members of the stack will be disabled.

To return the switch to stack membership, first connect to the switch via its console port, then run the `stack enable` command. Then save the configuration and run the `reboot` command. This will reboot the switch and it will re-join the stack as an ordinary member.

If the switch was previously the stack master, you might want to return it to its original stack master status. To do this you must run the `reboot` command again. This time—because the switch is now a stack member—the command will reboot the whole stack and result in a new master election.

Note the following when using the `no stack <stack-ID> enable` command:

- If the specified `stack-ID` is not used by any current stack member, the command will be rejected.

**CAUTION:** Disabling a stack member can significantly degrade the throughput capability of the stack.
STACKING COMMANDS
STACK ENABLE

**Example**
To turn on stacking on a stackable stand-alone unit, use the command:

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

**Related Commands**
reboot
license
stack management subnet

Overview
This command configures the subnet address used by the stack management VLAN.

Use the no variant of this command to reset the stack’s VLAN subnet management address back to the default address and mask (192.168.255.0/27).

Syntax
stack management subnet <ip-address>
no stack management subnet

Default
The default stacking management VLAN subnet address is 192.168.255.0 with a subnet mask 255.255.255.224 or /27.

Mode
Global Configuration

Usage
This command configures the stack management VLAN subnet address.

The management VLAN will be used for high speed communication between stacked units via the stacking ports. Although this command enables you to change the IP address command, the subnet mask must always remain as shown.

The stack management IP subnet is solely used internally to the stacked devices, and cannot be reached external to the stack. You should only change the stack management VLAN subnet address if it causes a conflict within your network.

Note that several separate stacks can use the same default management VLAN subnet address even though their user ports may share the same external network. If the stack subnet address is changed, then the configuration for any new units must also be updated before they are inserted into the stack.

If the management VLAN subnet address is changed by this command, you can use the no variant of this command to reset it to its default.

Example
To set the management VLAN subnet address to 192.168.255.144:

awplus# configure terminal
awplus(config)# stack management subnet 192.168.255.144

Related Commands
stack management vlan
### stack management vlan

#### Overview
Use this command to configure the stack management VLAN ID.

Use the **no** variant of this command to change the stack management VLAN ID back to the default (VLAN ID 4094).

#### Syntax
```
stack management vlan <2-4094>
no stack management vlan
```

#### Parameter | Description
---|---
<2-4094> | Stack management VLAN ID.

#### Default
VLAN ID 4094

#### Mode
Global Configuration

#### Usage
The management VLAN is used for high speed communication between stacked units. This command enables you to change the ID of this VLAN.

The default stacking management VLAN ID is 4094, which is the last configurable VLAN ID in the switch.

The stack management VLAN is created and configured automatically so that the stack VLAN cannot be used in the stack’s VLAN configuration commands (such as `awplus(config-vlan)# vlan <Stack management VLAN ID>`).

The management VLAN should only be changed if the default stack VLAN ID needs to be used in the stack’s VLAN configuration.

If the management VLAN ID is changed by this command, you can use the **no** variant of this command to change it back to default value.

**CAUTION:** If the management VLAN ID is changed by this command, you can use the **no** variant of this command to change it back to the default value.

When the command is entered, the updated management VLAN configuration will take effect once the stack is restarted.

#### Examples
To set the management VLAN to 4000, enter the following commands:
```
awplus# configure terminal
awplus(config)# stack management vlan 4000
```

To reset the management VLAN back to the default (4094), enter the following commands:
```
awplus# configure terminal
awplus(config)# no stack management vlan
```

#### Related Commands
- `stack management subnet`
Stacking Commands

Stack Priority

**Overview**
Use this command to change a specific stack member’s master-election priority.

**Syntax**
```
stack <stack-ID> priority <0-255>
no stack <stack-ID> priority
```

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;stack-ID&gt;</td>
<td>Stack member number, from 1 to 8.</td>
</tr>
<tr>
<td>priority</td>
<td>The stack member’s election priority value.</td>
</tr>
<tr>
<td>&lt;0-255&gt;</td>
<td>The stack member’s new priority value. The lowest value is assigned the highest priority. The default is 128.</td>
</tr>
</tbody>
</table>

**Mode**
Global Configuration

**Usage**
This command is used to change the value of a specific stack member's master-election priority. If the specified stack-ID is not used by any current stack member, the command will be rejected.

The election criteria selects the stack member with the lowest priority value to become the stack master. Where two stack members both have the same lowest priority value, then the stack member with the lowest MAC address will be elected as master.

**NOTE:** Assigning a new priority value will not immediately change the current stack master. In order to force a master re-election after the new priority value is assigned, use reboot stack-member <master's ID> to reboot the current stack master, a new stack master will then be elected based on the new priority values.

**Example**
To change the priority of stack member 2 to be 3, use the command:
```
awplus# configure terminal
awplus(config)# stack 2 priority 3
```

**Validation Command**
```
show stack
```
stack renumber

**Overview**  Use this command to renumber a specific stack member.

**Syntax**  
```
stack <existing stack-ID> renumber <new stack-ID>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;existing stack-ID&gt;</td>
<td>We recommend that you use only numbers 1 to 2 for a 2 unit stack, or 1 to 4 for a four unit stack.</td>
</tr>
<tr>
<td>renumber</td>
<td>Change the existing stack-ID.</td>
</tr>
<tr>
<td>&lt;new stack-ID&gt;</td>
<td>We recommend that you use only numbers 1 to 2 for a 2 unit stack, or 1 to 4 for a four unit stack.</td>
</tr>
</tbody>
</table>

**Default**  Every stack unit will initially try to use a stack-ID of 1.

**Mode**  Global Configuration

**Usage**  This command is used to change the ID of a specific stack member - primarily when exchanging stack members. The changes made by this command will not take effect until the switch is rebooted.

**NOTE:** This command does not alter any of the stack’s existing configuration, apart from the stack-ID specified. For example, if stack member 2 were removed from the stack and a new stack unit is assigned the member 2 stack-ID, then the interface configuration that existed for the removed stack member 2 will be applied to the new stack member 2.

The existing stack-ID must already be assigned to an existing stack member. To avoid duplicating IDs, a warning message will appear if you assign a new stack-ID that is currently assigned to another stack member. However, you can continue to renumber the stack-IDs and remove ID duplications. If you do not remove the duplications, then one of the devices will be forced to automatically renumber to an unused ID. Once you have removed any duplicate IDs, you can reboot the switch to implement your changes.

**NOTE:** The configured stack-ID is saved immediately on the renumbered member, and so is not reliant on using the copy running-config command for it to take effect.

**Example**  To renumber stack 1 to stack 2, use the commands:
```
awplus# configure terminal
awplus(config)# stack 1 renumber 2
```

**Validation Command**  show stack
Overview

This command is used to renumber the members of a stack so that their IDs are ordered sequentially, relative to the member’s physical position within the stack.

**CAUTION:** Changing the stack numbering will upset the existing stack member configurations such as port settings. This command is intended for use when the stack is either initially commissioned, or has undergone a major reconfiguration. In this situation you run the stack renumber command (which will automatically reboot the switch), then configure the stack members to meet the new requirements.

Syntax

```
stack <stack-ID> renumber cascade [<stack-ID>]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;stack-ID&gt;</td>
<td>The ID of the stack member to start renumbering from, from 1 to 8.</td>
</tr>
<tr>
<td>renumber</td>
<td>Change the existing stack-ID.</td>
</tr>
<tr>
<td>cascade</td>
<td>Renumber the existing stack-ID in cascade order.</td>
</tr>
<tr>
<td>&lt;stack-ID&gt;</td>
<td>The new ID for the first member renumbered, from 1 to 8.</td>
</tr>
</tbody>
</table>

Default

If no stack-ID is specified, the member will take the default ID of 1.

Mode

Global Configuration

Usage

This command is used to renumber the members of a stack so that their stack-IDs are ordered sequentially. This would normally be done either when the stack is initially configured or following a major reconfiguration.

The renumber will start on the specified stack member. If that stack-ID is not used by any of the existing stack member, the command will be rejected.

The starting stack member will be renumbered with the new stack-ID specified, or the default of member ID of 1. The stack-ID of the next physically will be the starting members ID +1, for example member ID 2. This renumbering will continue in cascading order around the stack members.

The changes will take place immediately and reboot all stack members. For this reason a confirmation prompt follows this command entry, asking whether you are sure you want to renumber and reboot the entire stack.

Example

```
awplus(config)# stack 1 renumber cascade

Any existing interface configuration may no longer be valid.
Are you sure you want to renumber and reboot the entire stack?(y/n): y
```
Related Commands

show stack
switch provision (stack)
stack renumber
Overview
This command configures the resiliency link used by the stack. The interface used may be either an eth port or a dedicated VLAN (resiliencylink VLAN) to which switch ports may become members. This VLAN is dedicated to the resiliency link function and must not be the stack management VLAN.

Syntax
```
stack resiliencylink <interface>
```
```
no stack resiliencylink
```

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface&gt;</td>
<td>The name of the interface that is connected to the resiliency link.</td>
</tr>
<tr>
<td></td>
<td>This may be either the eth port or the resiliencylink VLAN.</td>
</tr>
</tbody>
</table>

Mode
Global Configuration

Usage
The resiliency-link is only used when a backup member loses connectivity with the master via the stacking cables. Such a communication loss would occur if:

- a stacking link is removed or fails
- two or more stacking link cables are unplugged or fail
- the stack master itself fails due to a reboot or power failure

The resiliency-link allows the backup member to determine if the master is still present in the network by the reception of healthcheck messages sent by the master over the resiliency-link interface.

**CAUTION:** The purpose of the resiliency link is to enable the backup master to check the status of the master under fault conditions. If the resiliency link is not configured, and the master loses communication with its other stack member, then the stack will assume the master is NOT present in the network, which could cause network conflicts if the master is still online. Note that this is different to stacking operation in releases prior to version 5.3.1.

Reply healthcheck messages are received if the master is still online, but the stack will now split into two different “stubs”. The stub containing the existing master will continue operating as normal. The members in the masterless stub will now use a “type stack disabled-master” trigger to run a configuration to form a second temporary stack. This utilizes the remaining stack members’ resources without conflicting directly with the master’s configuration. If no “type stack disabled-master” trigger was configured on the switches, then the masterless stub members will disable their switch ports.

If no healthcheck messages are received, then the master is assumed to be completely offline, and so the other stack members can safely take over the master’s configuration.

**CAUTION:** The purpose of the resiliency link is to enable the stack members (particularly the backup master) to check the status of the master under fault conditions. If the resiliency link is not configured, and the master loses communication with its other
STACKING COMMANDS

STACK RESILIENCYLINK

stack members, then the stack will assume the master is NOT present in the network, which could cause network conflicts if the master is still online. Note that this is a change to the stacking of releases prior to version 5.3.1.

Example

To set the resiliency link to be VLAN 4093.

First use the stack resiliencylink command to create the resiliency vlan 4093

```
awplus# configure terminal
awplus(config)# stack resiliencylink vlan4093
```

Next use the switchport resiliencylink command to assign the resiliencylink vlan to the interface port, in this case port1.0.1.

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport resiliencylink
```

Related Commands

- show stack
- switch provision (stack)
- show stack resiliencylink
- stack disabled-master-monitoring
- switchport resiliencylink
**STACKING COMMANDS**

**STACK SOFTWARE-AUTO-SYNCHRONIZE**

---

**stack software-auto-synchronize**

**Overview**

This command re-enables the software version auto-synchronization feature either on a specified stack member or all stack members.

Use the **no** variant of this command to turn the software version auto-synchronization feature off.

**Syntax**

```
stack {all|<stack-ID>} software-auto-synchronize
no stack {all|<stack-ID>} software-auto-synchronize
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All stack members.</td>
</tr>
<tr>
<td>&lt;stack-ID&gt;</td>
<td>Stack member number, from 1 to 8.</td>
</tr>
</tbody>
</table>

**Default**

All the stack members have the stack software-auto-synchronize feature enabled by default.

**Mode**

Global Configuration

**Usage**

This command is used to enable the software version auto-synchronization feature for either a specific stack member or all stack members and candidates.

Note that if a device attempts to join a stack but is running a software release that is different to the other stack members, the software version auto-synchronization feature will copy the master’s software release onto the new member. If the software version auto-synchronization feature is not enabled, then the device will be unable to join the stack.

Note that the software version auto-synchronization feature may also result in the stack member downgrading its software release if the master is running an older software version.

**Examples**

To turn on the software-auto-synchronize feature on stack member 2, which was previously turned off, use the following commands:

```
awplus# configure terminal
awplus(config)# stack 2 software-auto-synchronize
```

To turn on the software-auto-synchronize feature for all stack members, which were previously turned off, use the following commands:

```
awplus# configure terminal
awplus(config)# stack all software-auto-synchronize
```

**Validation Command**

`show stack`
**stack virtual-chassis-id**

**Overview**  This command specifies the stack virtual chassis ID. The ID selected will determine which virtual MAC address the stack will use. The MAC address assigned to a stack must be unique within its network.

*NOTE:* The command will not take effect until the switch has been rebooted.

**Syntax**  `stack virtual-chassis-id <id>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;id&gt;</code></td>
<td>The value of the ID - enter a number in the range 0 to 4095.</td>
</tr>
</tbody>
</table>

**Mode**  Global Configuration

**Usage**  The virtual-chassis-id entered will form the last 12 bits of a pre-selected MAC prefix component; that is, `0000.cd37.0xxx`. If you enable the stack virtual MAC address feature (by using the `stack virtual-mac` command) without using the `stack virtual-chassis-id` command to select the virtual-chassis-id, then the stack will select a virtual-chassis-id from a number within the assigned range.

**Example**  To set the stack virtual-chassis-id to 63 use the commands

```
awplus# configure terminal
awplus(config)# stack virtual-chassis-id 63
```

This will result in a virtual MAC address of: `0000.cd37.003f`.

**Related Commands**

- `show running-config`
- `show stack`
- `switch provision (stack)`
- `stack virtual-mac`
STACKING COMMANDS
STACK VIRTUAL-MAC

stack virtual-mac

**Overview**  This command enables the stack virtual MAC address feature. For more information on this topic, see the VCStack Feature Overview and Configuration Guide. With this command set, the value applied for the virtual MAC address is determined by the setting of the command `stack virtual-chassis-id` command.

*CAUTION: Stack operation is only supported if stack virtual-mac is enabled.*

Before enabling the virtual MAC address feature, you should check that the stack’s virtual-chassis-id is not already used by another stack in the network. Otherwise the duplicate MAC addresses will cause problems for the network traffic.

**Syntax**

```
stack virtual-mac
no stack virtual mac
```

**Mode**  Global Configuration

**Usage**  Note that this command will not take effect until the switch has been rebooted.

**Example**

```
awplus# configure terminal
awplus(config)# stack virtual mac
```

**Related Commands**

- show running-config
- show stack
- switch provision (stack)
- stack virtual-chassis-id
switch provision (stack)

Overview
This command enables you to provide the configuration for a new stack member switch prior to physically connecting it to the stack. To run this command, the stack position must be vacant. The selected hardware type must be compatible existing stack hardware.

Use the no variant of this command to remove an existing switch provision.

Syntax
```
switch <stack-ID> {provision|reprovision} {x510-28|x510-52}
no switch <stack-ID> provision
```

Mode
Global Configuration

Usage
Note that although the syntax appears to allow provisioning on up to 8 stackable switches, in practice a maximum of 4 are configurable. Normally the stack members would be numbered 1 to 4, and so the command could be run to provision any stack member within this range; and we advise this procedure. In effect, the syntax then becomes:
```
switch <1-4> {provision|reprovision} {x510-28|x510-52}
```

However, you could number the stack units with any numbers between 1 and 8. For example you could number your four stack members 1, 2, 7 and 8. In this case you could provision any of the stack members within this range. We advise against numbering your stacks in this way.

Examples
To provision an x510-28 switch as stack member 3, use the following commands:
```
awplus# configure terminal
awplus(config)# switch 3 provision x510-28
```

To remove the provision of the x510-28 switch as stack member 3, use the following commands:
```
awplus# configure terminal
awplus(config)# no switch 3 provision
```
**switchport resiliencylink**

**Overview**  
This command configures the switch port to be a member of the stack resiliency link VLAN. Note that this switchport will only be used for stack resiliency-link traffic and will not perform any other function, or carry any other traffic.

The no variant of this command removes the switchport from the resiliency link VLAN.

**Syntax**  
switchport resiliencylink  
no switchport resiliencylink

**Mode**  
Interface Configuration

**Usage**  
Note that a resiliency link cannot be part of a static or dynamic aggregator group.

**Examples**  
To set the resiliency link to be VLAN 4093:

First, use the **stack resiliencylink** command to create the resiliency-link vlan vlan4093

```
awplus# configure terminal
awplus(config)# stack resiliencylink vlan4093
```

Next, use the **switchport resiliencylink** command to assign the resiliency-link vlan to the port, in this case port1.0.1.

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport resiliencylink
```

**Related Commands**  
stack resiliencylink  
show stack resiliencylink
STACKING COMMANDS
VLAN MODE STACK-LOCAL-VLAN

**vlan mode stack-local-vlan**

**Overview**  This command enables you to create stack-local-VLANs and use ICMP to monitor and diagnose issues within specific members of the stack. When a VLAN is added using this method, all its traffic will be trapped to and processed by the CPU of the specific local stack member, rather than the CPU of the stack master.

The **no** variant of this command destroys the specified VLAN.

**Syntax**  
```
vlan <vid> mode stack-local-vlan <member-id>
no vlan <vid>
```

**Parameter** | **Description**
---|---
<vid> | The VID of the VLAN to be created in the range 2-4094. We recommend that the first stack-local-vlan be assigned the number 4001 for the first stack member, then incremented by one for each stack member. So a stack of four members would be assigned the following VID numbers:
- stack member one: VID 4001
- stack member two: VID 4002
- stack member three: VID 4003
- stack member four: VID 4004

mode stack-local-vlan | Specifies that the new VLAN will function as a stack-local-VLAN.

<member-id> | Specifies the new stack member ID. Enter a decimal number in the range 1-8.

**Default**  By default, VLANs are automatically enabled as they are added.

**Mode**  VLAN Configuration

**Examples**  To add a stack-local-VLAN with the VID of 4002 and assign it to stack member 2, use the following commands:
```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 4002 mode stack-local-vlan 2
```

To remove VLAN 4002, use the following commands:
```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 4002
```

**Related Commands**  mtu

奄lan database
**Overview**  This command applies the functionality of the `no debug stack` command.
STACKING COMMANDS
UNDEBUG STACK