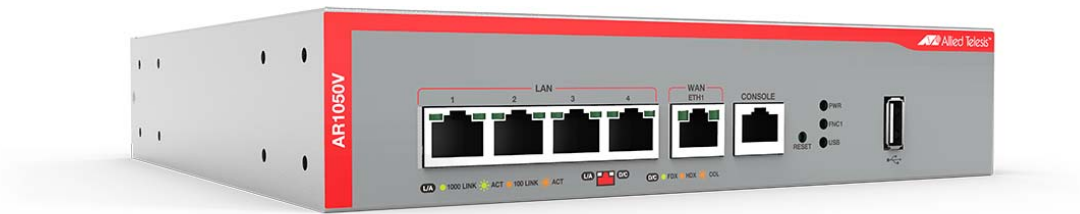


# AR1050V

## SECURE VIRTUAL PRIVATE NETWORK (VPN) ROUTER



# Command Reference for AlliedWare Plus™ Version 5.5.0-0.x

# Acknowledgments

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

Copyright ©1982, 1986, 1990, 1991, 1993 The Regents of the University of California.

All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For information about this see [www.openssl.org/](http://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](http://www.gnu.org/licenses/gpl2.html) and [www.gnu.org/licenses/gpl.html](http://www.gnu.org/licenses/gpl.html) respectively.

Source code for all GPL licensed software in this product can be obtained from the Allied Telesys GPL Code Download Center at: [www.alliedtelesys.com/support/](http://www.alliedtelesys.com/support/)

Allied Telesys 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 Telesys 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 Telesys Labs (Ltd)**  
**PO Box 8011**  
**Christchurch**  
**New Zealand**

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

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

© 2020 Allied Telesys, Inc.

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

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

---

# Contents

|                   |   |           |
|-------------------|---|-----------|
| <b>PART 1:</b>    | <b>Setup and Troubleshooting</b>                  | <b>49</b> |
| <b>Chapter 1:</b> | <b>CLI Navigation Commands</b>                    | <b>50</b> |
|                   | Introduction                                      | 50        |
|                   | configure terminal                                | 51        |
|                   | disable (Privileged Exec mode)                    | 52        |
|                   | do  | 53        |
|                   | enable (Privileged Exec mode)                     | 54        |
|                   | end   | 56        |
|                   | exit  | 57        |
|                   | help  | 58        |
|                   | logout  | 59        |
|                   | show history                                      | 60        |
| <b>Chapter 2:</b> | <b>File and Configuration Management Commands</b> | <b>61</b> |
|                   | Introduction                                      | 61        |
|                   | autoboot enable                                   | 64        |
|                   | boot config-file                                  | 65        |
|                   | boot config-file backup                           | 67        |
|                   | boot system                                       | 68        |
|                   | boot system backup                                | 69        |
|                   | cd  | 70        |
|                   | copy (filename)                                   | 71        |
|                   | copy current-software                             | 73        |
|                   | copy debug  | 74        |
|                   | copy running-config                               | 75        |
|                   | copy startup-config                               | 76        |
|                   | copy zmodem                                       | 77        |
|                   | create autoboot                                   | 78        |
|                   | delete  | 79        |
|                   | delete debug                                      | 80        |
|                   | dir   | 81        |
|                   | edit  | 83        |
|                   | edit (filename)                                   | 84        |

|   |     |
|---|-----|
| erase factory-default . . . . .         | .85 |
| erase startup-config . . . . .          | .86 |
| ip tftp source-interface . . . . .      | .87 |
| ipv6 tftp source-interface . . . . .    | .88 |
| mkdir . . . . .                         | .89 |
| move . . . . .                          | .90 |
| move debug . . . . .                    | .91 |
| pwd . . . . .                           | .92 |
| rmdir . . . . .                         | .93 |
| show autoboot . . . . .                 | .94 |
| show boot . . . . .                     | .95 |
| show file . . . . .                     | .97 |
| show file systems . . . . .             | .98 |
| show running-config . . . . .           | 100 |
| show running-config interface . . . . . | 103 |
| show startup-config . . . . .           | 106 |
| show version . . . . .                  | 107 |
| unmount . . . . .                       | 108 |
| write file . . . . .                    | 109 |
| write memory . . . . .                  | 110 |
| write terminal . . . . .                | 111 |

**Chapter 3: User Access Commands . . . . . 112**

|  |     |
|--|-----|
| Introduction . . . . .                                   | 112 |
| aaa authentication enable default local . . . . .        | 114 |
| aaa local authentication attempts lockout-time . . . . . | 115 |
| aaa local authentication attempts max-fail . . . . .     | 116 |
| aaa login fail-delay . . . . .                           | 117 |
| clear aaa local user lockout . . . . .                   | 118 |
| clear line console . . . . .                             | 119 |
| clear line vty . . . . .                                 | 120 |
| enable password . . . . .                                | 121 |
| enable secret . . . . .                                  | 124 |
| exec-timeout . . . . .                                   | 127 |
| flowcontrol hardware (asyn/console) . . . . .            | 129 |
| length (asyn) . . . . .                                  | 131 |
| line . . . . .   | 132 |
| privilege level . . . . .                                | 134 |
| security-password history . . . . .                      | 135 |
| security-password forced-change . . . . .                | 136 |
| security-password lifetime . . . . .                     | 137 |
| security-password min-lifetime-enforce . . . . .         | 138 |
| security-password minimum-categories . . . . .           | 139 |
| security-password minimum-length . . . . .               | 140 |
| security-password reject-expired-pwd . . . . .           | 141 |
| security-password warning . . . . .                      | 142 |
| service advanced-vty . . . . .                           | 143 |
| service password-encryption . . . . .                    | 144 |
| service telnet . . . . .                                 | 145 |
| show aaa local user locked . . . . .                     | 146 |
| show privilege . . . . .                                 | 147 |
| show security-password configuration . . . . .           | 148 |
| show security-password user . . . . .                    | 149 |

|                   |   |            |
|-------------------|---|------------|
|                   | show telnet . . . . .   | 150        |
|                   | show users . . . . .  | 151        |
|                   | telnet server . . . . .                                       | 152        |
|                   | terminal length . . . . .                                     | 153        |
|                   | terminal resize . . . . .                                     | 154        |
|                   | username . . . . .  | 155        |
| <b>Chapter 4:</b> | <b>GUI Commands . . . . .</b>                                 | <b>157</b> |
|                   | Introduction . . . . .  | 157        |
|                   | atmf topology-gui enable . . . . .                            | 158        |
|                   | http port . . . . .   | 159        |
|                   | http secure-port . . . . .                                    | 160        |
|                   | log event-host . . . . .                                      | 161        |
|                   | service http . . . . .  | 162        |
|                   | show http . . . . .   | 163        |
|                   | update webgui now . . . . .                                   | 164        |
| <b>Chapter 5:</b> | <b>Update Manager Commands . . . . .</b>                      | <b>165</b> |
|                   | Introduction . . . . .  | 165        |
|                   | show resource . . . . .                                       | 166        |
|                   | update now . . . . .  | 167        |
|                   | update webgui now . . . . .                                   | 168        |
| <b>Chapter 6:</b> | <b>System Configuration and Monitoring Commands . . . . .</b> | <b>169</b> |
|                   | Introduction . . . . .  | 169        |
|                   | banner exec . . . . .   | 171        |
|                   | banner login (system) . . . . .                               | 173        |
|                   | banner motd . . . . .   | 175        |
|                   | clock set . . . . .   | 177        |
|                   | clock summer-time date . . . . .                              | 178        |
|                   | clock summer-time recurring . . . . .                         | 180        |
|                   | clock timezone . . . . .                                      | 182        |
|                   | debug core-file . . . . .                                     | 183        |
|                   | hostname . . . . .  | 184        |
|                   | max-fib-routes . . . . .                                      | 186        |
|                   | max-static-routes . . . . .                                   | 187        |
|                   | no debug all . . . . .  | 188        |
|                   | reboot . . . . .  | 190        |
|                   | receive-packet-scheduler . . . . .                            | 191        |
|                   | reload . . . . .  | 193        |
|                   | show clock . . . . .  | 194        |
|                   | show cpu . . . . .  | 196        |
|                   | show cpu history . . . . .                                    | 199        |
|                   | show debugging . . . . .                                      | 201        |
|                   | show interface memory . . . . .                               | 202        |
|                   | show memory . . . . .   | 204        |
|                   | show memory allocations . . . . .                             | 206        |
|                   | show memory history . . . . .                                 | 208        |
|                   | show memory pools . . . . .                                   | 209        |
|                   | show memory shared . . . . .                                  | 210        |
|                   | show process . . . . .  | 211        |
|                   | show reboot history . . . . .                                 | 213        |

|                                    |     |
|------------------------------------|-----|
| show router-id . . . . .           | 214 |
| show system . . . . .              | 215 |
| show system interrupts . . . . .   | 216 |
| show system mac . . . . .          | 217 |
| show system pci device . . . . .   | 218 |
| show system pci tree . . . . .     | 219 |
| show system serialnumber . . . . . | 220 |
| show tech-support . . . . .        | 221 |
| speed (asyn) . . . . .             | 223 |
| terminal monitor . . . . .         | 225 |
| undebg all . . . . .               | 226 |

**Chapter 7: Logging Commands . . . . . 227**

|                                  |     |
|----------------------------------|-----|
| Introduction . . . . .           | 227 |
| clear exception log . . . . .    | 230 |
| clear log . . . . .              | 231 |
| clear log buffered . . . . .     | 232 |
| clear log external . . . . .     | 233 |
| clear log permanent . . . . .    | 234 |
| connection-log events . . . . .  | 235 |
| copy buffered-log . . . . .      | 236 |
| copy permanent-log . . . . .     | 237 |
| default log buffered . . . . .   | 238 |
| default log console . . . . .    | 239 |
| default log email . . . . .      | 240 |
| default log external . . . . .   | 241 |
| default log host . . . . .       | 242 |
| default log monitor . . . . .    | 243 |
| default log permanent . . . . .  | 244 |
| log buffered . . . . .           | 245 |
| log buffered (filter) . . . . .  | 246 |
| log buffered exclude . . . . .   | 249 |
| log buffered size . . . . .      | 252 |
| log console . . . . .            | 253 |
| log console (filter) . . . . .   | 254 |
| log console exclude . . . . .    | 257 |
| log date-format . . . . .        | 260 |
| log email . . . . .              | 261 |
| log email (filter) . . . . .     | 262 |
| log email exclude . . . . .      | 265 |
| log email time . . . . .         | 268 |
| log external . . . . .           | 270 |
| log external (filter) . . . . .  | 272 |
| log external exclude . . . . .   | 275 |
| log external rotate . . . . .    | 278 |
| log external size . . . . .      | 280 |
| log facility . . . . .           | 281 |
| log host . . . . .               | 283 |
| log host (filter) . . . . .      | 285 |
| log host exclude . . . . .       | 288 |
| log host source . . . . .        | 291 |
| log host startup-delay . . . . . | 292 |
| log host time . . . . .          | 294 |

|                    |   |            |
|--------------------|---|------------|
|                    | log monitor (filter) . . . . .                  | 296        |
|                    | log monitor exclude . . . . .                   | 299        |
|                    | log permanent . . . . .                         | 302        |
|                    | log permanent (filter) . . . . .                | 303        |
|                    | log permanent exclude . . . . .                 | 306        |
|                    | log permanent size . . . . .                    | 309        |
|                    | log-rate-limit nsm . . . . .                    | 310        |
|                    | log trustpoint . . . . .                        | 311        |
|                    | log url-requests . . . . .                      | 312        |
|                    | show connection-log events . . . . .            | 313        |
|                    | show counter log . . . . .                      | 314        |
|                    | show exception log . . . . .                    | 315        |
|                    | show log . . . . .                              | 316        |
|                    | show log config . . . . .                       | 318        |
|                    | show log external . . . . .                     | 320        |
|                    | show log permanent . . . . .                    | 321        |
|                    | show running-config log . . . . .               | 322        |
|                    | unmount . . . . .                               | 323        |
| <b>Chapter 8:</b>  | <b>Scripting Commands . . . . .</b>             | <b>324</b> |
|                    | Introduction . . . . .                          | 324        |
|                    | activate . . . . .                              | 325        |
|                    | echo . . . . .                                  | 326        |
|                    | wait . . . . .                                  | 327        |
| <b>Chapter 9:</b>  | <b>Interface Commands . . . . .</b>             | <b>328</b> |
|                    | Introduction . . . . .                          | 328        |
|                    | description (interface) . . . . .               | 329        |
|                    | interface (to configure) . . . . .              | 330        |
|                    | ip tcp adjust-mss . . . . .                     | 332        |
|                    | ipv6 tcp adjust-mss . . . . .                   | 334        |
|                    | mru jumbo . . . . .                             | 336        |
|                    | mtu . . . . .                                   | 337        |
|                    | service statistics interfaces counter . . . . . | 339        |
|                    | show interface . . . . .                        | 340        |
|                    | show interface brief . . . . .                  | 344        |
|                    | show interface memory . . . . .                 | 345        |
|                    | show interface status . . . . .                 | 347        |
|                    | shutdown . . . . .                              | 349        |
| <b>Chapter 10:</b> | <b>USB Cellular Modem Commands . . . . .</b>    | <b>350</b> |
|                    | Introduction . . . . .                          | 350        |
|                    | apn . . . . .                                   | 351        |
|                    | chat-script . . . . .                           | 353        |
|                    | cid . . . . .                                   | 354        |
|                    | encapsulation ppp . . . . .                     | 355        |
|                    | show cellular . . . . .                         | 356        |
|                    | show system usb . . . . .                       | 359        |
|                    | usb mode-switch . . . . .                       | 361        |
| <b>PART 2:</b>     | <b>Interfaces and Layer 2 . . . . .</b>         | <b>363</b> |

|                    |   |            |
|--------------------|---|------------|
| <b>Chapter 11:</b> | <b>Switching Commands</b> . . . . .       | <b>364</b> |
|                    | Introduction . . . . .                    | 364        |
|                    | backpressure . . . . .                    | 366        |
|                    | clear mac address-table dynamic . . . . . | 368        |
|                    | clear mac address-table static . . . . .  | 369        |
|                    | clear port counter . . . . .              | 370        |
|                    | debug platform packet . . . . .           | 371        |
|                    | duplex . . . . .                          | 373        |
|                    | flowcontrol (switch port) . . . . .       | 374        |
|                    | linkflap action . . . . .                 | 376        |
|                    | mac address-table acquire . . . . .       | 377        |
|                    | mac address-table ageing-time . . . . .   | 378        |
|                    | mac address-table static . . . . .        | 379        |
|                    | polarity . . . . .                        | 380        |
|                    | show debugging platform packet . . . . .  | 381        |
|                    | show flowcontrol interface . . . . .      | 382        |
|                    | show interface err-disabled . . . . .     | 383        |
|                    | show interface switchport . . . . .       | 384        |
|                    | show mac address-table . . . . .          | 385        |
|                    | show platform . . . . .                   | 387        |
|                    | show platform port . . . . .              | 389        |
|                    | show storm-control . . . . .              | 391        |
|                    | speed . . . . .                           | 392        |
|                    | storm-control level . . . . .             | 394        |
|                    | undebug platform packet . . . . .         | 395        |
| <br>               |   |            |
| <b>Chapter 12:</b> | <b>Bridging Commands</b> . . . . .        | <b>396</b> |
|                    | Introduction . . . . .                    | 396        |
|                    | ageing-time . . . . .                     | 398        |
|                    | bridge . . . . .                          | 399        |
|                    | bridge-group . . . . .                    | 400        |
|                    | clear mac-filter counter . . . . .        | 401        |
|                    | default-action . . . . .                  | 402        |
|                    | default-protocol-action . . . . .         | 404        |
|                    | l3-filtering enable . . . . .             | 405        |
|                    | mac-filter-group egress . . . . .         | 406        |
|                    | mac-filter . . . . .                      | 407        |
|                    | mac-filter-group . . . . .                | 408        |
|                    | mac-learning . . . . .                    | 409        |
|                    | protocol ethii (macfilter) . . . . .      | 410        |
|                    | protocol novell (macfilter) . . . . .     | 412        |
|                    | protocol sap (macfilter) . . . . .        | 414        |
|                    | protocol snap (macfilter) . . . . .       | 416        |
|                    | rule (macfilter) . . . . .                | 418        |
|                    | rule ip (macfilter) . . . . .             | 420        |
|                    | rule ipv6 (macfilter) . . . . .           | 422        |
|                    | show bridge . . . . .                     | 424        |
|                    | show bridge macaddr . . . . .             | 426        |
|                    | show mac-filter . . . . .                 | 427        |
| <br>               |   |            |
| <b>Chapter 13:</b> | <b>PPP Commands</b> . . . . .             | <b>429</b> |
|                    | Introduction . . . . .                    | 429        |



|                           |     |
|---------------------------|-----|
| debug ppp                 | 431 |
| encapsulation ppp         | 434 |
| interface (PPP)           | 435 |
| ip address negotiated     | 436 |
| ip tcp adjust-mss         | 438 |
| ip unnumbered             | 440 |
| ipv6 tcp adjust-mss       | 442 |
| keepalive (PPP)           | 444 |
| mtu (PPP)                 | 446 |
| peer default ip address   | 447 |
| peer neighbor-route       | 449 |
| ppp authentication        | 451 |
| ppp authentication refuse | 453 |
| ppp hostname              | 455 |
| ppp ipcp dns              | 457 |
| ppp ipcp dns suffix-list  | 459 |
| ppp ipcp ip-override      | 461 |
| ppp password              | 462 |
| ppp service-name (PPPoE)  | 463 |
| ppp timeout idle          | 464 |
| ppp username              | 465 |
| show debugging ppp        | 466 |
| show interface (PPP)      | 467 |
| undebug ppp               | 471 |

**PART 3: Routing . . . . . 472**

**Chapter 14: IP Addressing and Protocol Commands . . . . . 473**

|   |     |
|---|-----|
| Introduction                            | 473 |
| arp-aging-timeout                       | 475 |
| arp                                     | 476 |
| arp log                                 | 477 |
| arp opportunistic-nd                    | 480 |
| arp-reply-bc-dmac                       | 481 |
| clear arp-cache                         | 482 |
| debug ip packet interface               | 483 |
| ip address (IP Addressing and Protocol) | 485 |
| ip directed-broadcast                   | 486 |
| ip forward-protocol udp                 | 488 |
| ip gratuitous-arp-link                  | 490 |
| ip helper-address                       | 492 |
| ip limited-local-proxy-arp              | 494 |
| ip local-proxy-arp                      | 496 |
| ip proxy-arp                            | 497 |
| ip redirects                            | 498 |
| ip tcp synack-retries                   | 499 |
| ip tcp timeout established              | 500 |
| ip unreachable                          | 501 |
| local-proxy-arp                         | 503 |
| optimistic-nd                           | 504 |
| ping                                    | 505 |
| show arp                                | 506 |

|                                      |     |
|--------------------------------------|-----|
| show debugging ip packet . . . . .   | 507 |
| show ip flooding-nexthops . . . . .  | 508 |
| show ip interface . . . . .          | 509 |
| show ip sockets . . . . .            | 510 |
| show ip traffic . . . . .            | 513 |
| tcpdump . . . . .                    | 515 |
| traceroute . . . . .                 | 516 |
| undebg ip packet interface . . . . . | 517 |

**Chapter 15: Domain Name Service (DNS) Commands . . . . . 518**

|  |     |
|--|-----|
| Introduction . . . . .                       | 518 |
| accept-invalid-sslcrt . . . . .              | 520 |
| clear ip dns forwarding cache . . . . .      | 521 |
| ddns enable . . . . .                        | 522 |
| ddns-update-method . . . . .                 | 523 |
| ddns-update now . . . . .                    | 524 |
| debug ddns . . . . .                         | 525 |
| debug ip dns forwarding . . . . .            | 526 |
| description (Domain List) . . . . .          | 527 |
| domain (Domain List) . . . . .               | 528 |
| host-name (DDNS) . . . . .                   | 529 |
| ip ddns-update-method . . . . .              | 530 |
| ip dns forwarding . . . . .                  | 531 |
| ip dns forwarding cache . . . . .            | 532 |
| ip dns forwarding dead-time . . . . .        | 533 |
| ip dns forwarding domain-list . . . . .      | 534 |
| ip dns forwarding retry . . . . .            | 535 |
| ip dns forwarding source-interface . . . . . | 536 |
| ip dns forwarding timeout . . . . .          | 537 |
| ip domain-list . . . . .                     | 538 |
| ip domain-lookup . . . . .                   | 539 |
| ip domain-name . . . . .                     | 541 |
| ip name-server . . . . .                     | 542 |
| ip name-server preferred-order . . . . .     | 544 |
| ipv6 ddns-update-method . . . . .            | 545 |
| password (DDNS) . . . . .                    | 546 |
| ppp ipcp dns . . . . .                       | 547 |
| ppp ipcp dns suffix-list . . . . .           | 549 |
| retry-interval (DDNS) . . . . .              | 551 |
| show ddns-update-method status . . . . .     | 552 |
| show debugging ip dns forwarding . . . . .   | 553 |
| show hosts . . . . .                         | 554 |
| show ip dns forwarding . . . . .             | 555 |
| show ip dns forwarding cache . . . . .       | 556 |
| show ip dns forwarding server . . . . .      | 557 |
| show ip domain-list . . . . .                | 558 |
| show ip domain-name . . . . .                | 559 |
| show ip name-server . . . . .                | 560 |
| suppress-ipv4-updates (DDNS) . . . . .       | 561 |
| undebg (DDNS) . . . . .                      | 562 |
| update-interval (DDNS) . . . . .             | 563 |
| update-url (DDNS) . . . . .                  | 564 |
| use-ipv4-for-ipv6-updates (DDNS) . . . . .   | 567 |

|                    |   |            |
|--------------------|---|------------|
|                    | username (DDNS) . . . . .                           | 568        |
| <b>Chapter 16:</b> | <b>IPv6 Commands . . . . .</b>                      | <b>569</b> |
|                    | Introduction . . . . .                              | 569        |
|                    | clear ipv6 neighbors . . . . .                      | 571        |
|                    | ipv6 address . . . . .                              | 572        |
|                    | ipv6 address autoconfig . . . . .                   | 574        |
|                    | ipv6 address suffix . . . . .                       | 576        |
|                    | ipv6 enable . . . . .                               | 577        |
|                    | ipv6 eui64-linklocal . . . . .                      | 579        |
|                    | ipv6 forwarding . . . . .                           | 580        |
|                    | ipv6 nd accept-ra-pinfo . . . . .                   | 581        |
|                    | ipv6 nd current-hoplimit . . . . .                  | 582        |
|                    | ipv6 nd managed-config-flag . . . . .               | 584        |
|                    | ipv6 nd minimum-ra-interval . . . . .               | 585        |
|                    | ipv6 nd other-config-flag . . . . .                 | 587        |
|                    | ipv6 nd prefix . . . . .                            | 588        |
|                    | ipv6 nd proxy interface . . . . .                   | 590        |
|                    | ipv6 nd ra-interval . . . . .                       | 591        |
|                    | ipv6 nd ra-lifetime . . . . .                       | 592        |
|                    | ipv6 nd reachable-time . . . . .                    | 593        |
|                    | ipv6 nd retransmission-time . . . . .               | 595        |
|                    | ipv6 nd suppress-ra . . . . .                       | 597        |
|                    | ipv6 neighbor . . . . .                             | 598        |
|                    | ipv6 opportunistic-nd . . . . .                     | 599        |
|                    | ipv6 route . . . . .                                | 600        |
|                    | ipv6 unreachable . . . . .                          | 601        |
|                    | optimistic-nd . . . . .                             | 602        |
|                    | ping ipv6 . . . . .                                 | 603        |
|                    | show ipv6 forwarding . . . . .                      | 605        |
|                    | show ipv6 interface brief . . . . .                 | 606        |
|                    | show ipv6 neighbors . . . . .                       | 607        |
|                    | show ipv6 route . . . . .                           | 608        |
|                    | show ipv6 route summary . . . . .                   | 609        |
|                    | traceroute ipv6 . . . . .                           | 610        |
| <b>Chapter 17:</b> | <b>Routing Commands . . . . .</b>                   | <b>611</b> |
|                    | Introduction . . . . .                              | 611        |
|                    | ip route . . . . .                                  | 612        |
|                    | ipv6 route . . . . .                                | 614        |
|                    | max-fib-routes . . . . .                            | 615        |
|                    | max-static-routes . . . . .                         | 616        |
|                    | maximum-paths . . . . .                             | 617        |
|                    | show ip route . . . . .                             | 618        |
|                    | show ip route database . . . . .                    | 620        |
|                    | show ip route summary . . . . .                     | 621        |
|                    | show ipv6 route . . . . .                           | 622        |
|                    | show ipv6 route summary . . . . .                   | 623        |
| <b>PART 4:</b>     | <b>Access and Security . . . . .</b>                | <b>624</b> |
| <b>Chapter 18:</b> | <b>Public Key Infrastructure Commands . . . . .</b> | <b>625</b> |

|                              |     |
|------------------------------|-----|
| Introduction                 | 625 |
| crypto key generate rsa      | 626 |
| crypto key zeroize           | 627 |
| crypto pki authenticate      | 628 |
| crypto pki enroll            | 629 |
| crypto pki export pem        | 630 |
| crypto pki export pkcs12     | 631 |
| crypto pki import pem        | 632 |
| crypto pki import pkcs12     | 634 |
| crypto pki trustpoint        | 635 |
| enrollment (ca-trustpoint)   | 636 |
| fingerprint (ca-trustpoint)  | 637 |
| no crypto pki certificate    | 639 |
| rsakeypair (ca-trustpoint)   | 640 |
| show crypto key mypubkey rsa | 641 |
| show crypto pki certificates | 642 |
| show crypto pki trustpoint   | 644 |
| subject-name (ca-trustpoint) | 645 |

**PART 5: Network Management . . . . . 647**

**Chapter 19: Allied Telesis Management Framework™ (AMF) Commands . . . . . 648**

|  |     |
|--|-----|
| Introduction                                     | 648 |
| application-proxy ip-filter                      | 653 |
| application-proxy quarantine-vlan                | 654 |
| application-proxy redirect-url                   | 655 |
| application-proxy threat-protection              | 656 |
| application-proxy threat-protection send-summary | 657 |
| application-proxy whitelist enable               | 658 |
| application-proxy whitelist server               | 659 |
| area-link  | 661 |
| atmf area  | 663 |
| atmf area password                               | 665 |
| atmf authorize                                   | 667 |
| atmf authorize provision                         | 669 |
| atmf backup                                      | 671 |
| atmf backup area-masters delete                  | 672 |
| atmf backup area-masters enable                  | 673 |
| atmf backup area-masters now                     | 674 |
| atmf backup area-masters synchronize             | 675 |
| atmf backup bandwidth                            | 676 |
| atmf backup delete                               | 677 |
| atmf backup enable                               | 678 |
| atmf backup guests delete                        | 679 |
| atmf backup guests enable                        | 680 |
| atmf backup guests now                           | 681 |
| atmf backup guests synchronize                   | 682 |
| atmf backup now                                  | 683 |
| atmf backup redundancy enable                    | 685 |
| atmf backup server                               | 686 |
| atmf backup stop                                 | 688 |
| atmf backup synchronize                          | 689 |

---

|   |     |
|---|-----|
| atmf cleanup . . . . .                              | 690 |
| atmf container . . . . .                            | 691 |
| atmf container login . . . . .                      | 692 |
| atmf controller . . . . .                           | 693 |
| atmf distribute firmware . . . . .                  | 694 |
| atmf domain vlan . . . . .                          | 696 |
| atmf enable . . . . .                               | 699 |
| atmf group (membership) . . . . .                   | 700 |
| atmf guest-class . . . . .                          | 702 |
| atmf log-verbose . . . . .                          | 704 |
| atmf management subnet . . . . .                    | 705 |
| atmf management vlan . . . . .                      | 708 |
| atmf master . . . . .                               | 710 |
| atmf mtu . . . . .                                  | 711 |
| atmf network-name . . . . .                         | 712 |
| atmf provision (interface) . . . . .                | 713 |
| atmf provision node . . . . .                       | 714 |
| atmf reboot-rolling . . . . .                       | 716 |
| atmf recover . . . . .                              | 720 |
| atmf recover guest . . . . .                        | 722 |
| atmf recover led-off . . . . .                      | 723 |
| atmf recovery-server . . . . .                      | 724 |
| atmf remote-login . . . . .                         | 726 |
| atmf restricted-login . . . . .                     | 728 |
| atmf secure-mode . . . . .                          | 730 |
| atmf secure-mode certificate expire . . . . .       | 732 |
| atmf secure-mode certificate expiry . . . . .       | 733 |
| atmf secure-mode certificate renew . . . . .        | 734 |
| atmf secure-mode enable-all . . . . .               | 735 |
| atmf select-area . . . . .                          | 737 |
| atmf topology-gui enable . . . . .                  | 738 |
| atmf trustpoint . . . . .                           | 739 |
| atmf virtual-crosslink . . . . .                    | 741 |
| atmf virtual-link . . . . .                         | 743 |
| atmf virtual-link protection . . . . .              | 746 |
| atmf working-set . . . . .                          | 748 |
| bridge-group . . . . .                              | 750 |
| clear application-proxy threat-protection . . . . . | 751 |
| clear atmf links . . . . .                          | 752 |
| clear atmf links virtual . . . . .                  | 753 |
| clear atmf links statistics . . . . .               | 754 |
| clear atmf recovery-file . . . . .                  | 755 |
| clear atmf secure-mode certificates . . . . .       | 756 |
| clear atmf secure-mode statistics . . . . .         | 757 |
| clone (amf-provision) . . . . .                     | 758 |
| configure boot config (amf-provision) . . . . .     | 760 |
| configure boot system (amf-provision) . . . . .     | 762 |
| copy (amf-provision) . . . . .                      | 764 |
| create (amf-provision) . . . . .                    | 765 |
| debug atmf . . . . .                                | 767 |
| debug atmf packet . . . . .                         | 769 |
| delete (amf-provision) . . . . .                    | 772 |
| discovery . . . . .                                 | 774 |

---

|   |     |
|---|-----|
| description (amf-container) . . . . .                 | 776 |
| erase factory-default . . . . .                       | 777 |
| http-enable . . . . .                                 | 778 |
| identity (amf-provision) . . . . .                    | 780 |
| license-cert (amf-provision) . . . . .                | 782 |
| locate (amf-provision) . . . . .                      | 784 |
| log event-host . . . . .                              | 786 |
| modeltype . . . . .                                   | 787 |
| service atmf-application-proxy . . . . .              | 788 |
| show application-proxy threat-protection . . . . .    | 789 |
| show application-proxy whitelist interface . . . . .  | 791 |
| show application-proxy whitelist server . . . . .     | 793 |
| show application-proxy whitelist supplicant . . . . . | 794 |
| show atmf . . . . .                                   | 796 |
| show atmf area . . . . .                              | 800 |
| show atmf area guests . . . . .                       | 803 |
| show atmf area guests-detail . . . . .                | 805 |
| show atmf area nodes . . . . .                        | 807 |
| show atmf area nodes-detail . . . . .                 | 809 |
| show atmf area summary . . . . .                      | 811 |
| show atmf authorization . . . . .                     | 812 |
| show atmf backup . . . . .                            | 815 |
| show atmf backup area . . . . .                       | 819 |
| show atmf backup guest . . . . .                      | 821 |
| show atmf container . . . . .                         | 823 |
| show atmf detail . . . . .                            | 826 |
| show atmf group . . . . .                             | 828 |
| show atmf group members . . . . .                     | 830 |
| show atmf guests . . . . .                            | 832 |
| show atmf guests detail . . . . .                     | 834 |
| show atmf links . . . . .                             | 837 |
| show atmf links detail . . . . .                      | 839 |
| show atmf links guest . . . . .                       | 848 |
| show atmf links guest detail . . . . .                | 850 |
| show atmf links statistics . . . . .                  | 854 |
| show atmf nodes . . . . .                             | 857 |
| show atmf provision nodes . . . . .                   | 859 |
| show atmf recovery-file . . . . .                     | 861 |
| show atmf secure-mode . . . . .                       | 862 |
| show atmf secure-mode audit . . . . .                 | 864 |
| show atmf secure-mode audit link . . . . .            | 865 |
| show atmf secure-mode certificates . . . . .          | 866 |
| show atmf secure-mode sa . . . . .                    | 869 |
| show atmf secure-mode statistics . . . . .            | 872 |
| show atmf tech . . . . .                              | 874 |
| show atmf virtual-links . . . . .                     | 877 |
| show atmf working-set . . . . .                       | 879 |
| show debugging atmf . . . . .                         | 880 |
| show debugging atmf packet . . . . .                  | 881 |
| show running-config atmf . . . . .                    | 882 |
| state . . . . .                                       | 883 |
| switchport atmf-agentlink . . . . .                   | 885 |
| switchport atmf-arealink remote-area . . . . .        | 886 |

|                                     |     |
|-------------------------------------|-----|
| switchport atmf-crosslink . . . . . | 888 |
| switchport atmf-guestlink . . . . . | 890 |
| switchport atmf-link . . . . .      | 892 |
| type atmf node . . . . .            | 893 |
| undebug atmf . . . . .              | 896 |
| username . . . . .                  | 897 |

**Chapter 20: Dynamic Host Configuration Protocol (DHCP) Commands . . . . . 899**

|  |     |
|--|-----|
| Introduction . . . . .                                       | 899 |
| bootfile . . . . .   | 901 |
| clear ip dhcp binding . . . . .                              | 902 |
| default-router . . . . .                                     | 903 |
| dns-server . . . . .   | 904 |
| domain-name . . . . .  | 905 |
| host (DHCP) . . . . .  | 906 |
| ip address dhcp . . . . .                                    | 907 |
| ip dhcp bootp ignore . . . . .                               | 909 |
| ip dhcp leasequery enable . . . . .                          | 910 |
| ip dhcp option . . . . .                                     | 911 |
| ip dhcp pool . . . . .                                       | 913 |
| ip dhcp-client default-route distance . . . . .              | 914 |
| ip dhcp-client request vendor-identifying-specific . . . . . | 916 |
| ip dhcp-client vendor-identifying-class . . . . .            | 917 |
| ip dhcp-relay agent-option . . . . .                         | 918 |
| ip dhcp-relay agent-option checking . . . . .                | 920 |
| ip dhcp-relay agent-option remote-id . . . . .               | 922 |
| ip dhcp-relay information policy . . . . .                   | 924 |
| ip dhcp-relay maxhops . . . . .                              | 926 |
| ip dhcp-relay max-message-length . . . . .                   | 927 |
| ip dhcp-relay server-address . . . . .                       | 929 |
| ip dhcp-relay use-client-side-address . . . . .              | 931 |
| lease . . . . .  | 933 |
| network (DHCP) . . . . .                                     | 935 |
| next-server . . . . .  | 936 |
| option . . . . .   | 937 |
| probe enable . . . . .                                       | 939 |
| probe packets . . . . .                                      | 940 |
| probe timeout . . . . .                                      | 941 |
| probe type . . . . .   | 942 |
| range . . . . .  | 943 |
| route . . . . .  | 944 |
| service dhcp-relay . . . . .                                 | 945 |
| service dhcp-server . . . . .                                | 946 |
| short-lease-threshold . . . . .                              | 947 |
| show counter dhcp-client . . . . .                           | 949 |
| show counter dhcp-relay . . . . .                            | 950 |
| show counter dhcp-server . . . . .                           | 953 |
| show dhcp lease . . . . .                                    | 955 |
| show ip dhcp binding . . . . .                               | 956 |
| show ip dhcp pool . . . . .                                  | 958 |
| show ip dhcp-relay . . . . .                                 | 963 |
| show ip dhcp server statistics . . . . .                     | 964 |
| show ip dhcp server summary . . . . .                        | 966 |

|                       |     |
|-----------------------|-----|
| subnet-mask . . . . . | 967 |
|-----------------------|-----|

**Chapter 21: DHCP for IPv6 (DHCPv6) Commands . . . . . 968**

|  |      |
|--|------|
| Introduction . . . . .                         | 968  |
| address prefix . . . . .                       | 970  |
| address range . . . . .                        | 972  |
| clear counter ipv6 dhcp-client . . . . .       | 974  |
| clear counter ipv6 dhcp-server . . . . .       | 975  |
| clear ipv6 dhcp binding . . . . .              | 976  |
| clear ipv6 dhcp client . . . . .               | 978  |
| dns-server (DHCPv6) . . . . .                  | 979  |
| domain-name (DHCPv6) . . . . .                 | 981  |
| ip dhcp-relay agent-option . . . . .           | 982  |
| ip dhcp-relay agent-option checking . . . . .  | 984  |
| ip dhcp-relay agent-option remote-id . . . . . | 986  |
| ip dhcp-relay information policy . . . . .     | 988  |
| ip dhcp-relay maxhops . . . . .                | 990  |
| ip dhcp-relay max-message-length . . . . .     | 991  |
| ip dhcp-relay server-address . . . . .         | 993  |
| ipv6 address (DHCPv6 PD) . . . . .             | 995  |
| ipv6 address dhcp . . . . .                    | 998  |
| ipv6 dhcp client pd . . . . .                  | 1000 |
| ipv6 dhcp option . . . . .                     | 1002 |
| ipv6 dhcp pool . . . . .                       | 1004 |
| ipv6 dhcp server . . . . .                     | 1006 |
| ipv6 local pool . . . . .                      | 1007 |
| ipv6 nd prefix (DHCPv6) . . . . .              | 1009 |
| link-address . . . . .                         | 1011 |
| option (DHCPv6) . . . . .                      | 1013 |
| prefix-delegation pool . . . . .               | 1015 |
| service dhcp-relay . . . . .                   | 1017 |
| show counter dhcp-relay . . . . .              | 1018 |
| show counter ipv6 dhcp-client . . . . .        | 1021 |
| show counter ipv6 dhcp-server . . . . .        | 1023 |
| show ip dhcp-relay . . . . .                   | 1025 |
| show ipv6 dhcp . . . . .                       | 1026 |
| show ipv6 dhcp binding . . . . .               | 1027 |
| show ipv6 dhcp interface . . . . .             | 1030 |
| show ipv6 dhcp pool . . . . .                  | 1032 |
| sntp-address . . . . .                         | 1034 |

**Chapter 22: NTP Commands . . . . . 1035**

|                                  |      |
|----------------------------------|------|
| Introduction . . . . .           | 1035 |
| ntp authenticate . . . . .       | 1036 |
| ntp authentication-key . . . . . | 1037 |
| ntp broadcastdelay . . . . .     | 1038 |
| ntp discard . . . . .            | 1039 |
| ntp master . . . . .             | 1040 |
| ntp peer . . . . .               | 1041 |
| ntp rate-limit . . . . .         | 1043 |
| ntp restrict . . . . .           | 1044 |
| ntp server . . . . .             | 1046 |



|                    |  |             |
|--------------------|--|-------------|
|                    | ntp source . . . . .                         | 1048        |
|                    | ntp trusted-key (deprecated) . . . . .       | 1050        |
|                    | show counter ntp (deprecated) . . . . .      | 1051        |
|                    | show ntp associations . . . . .              | 1052        |
|                    | show ntp counters . . . . .                  | 1054        |
|                    | show ntp counters associations . . . . .     | 1055        |
|                    | show ntp status . . . . .                    | 1056        |
| <b>Chapter 23:</b> | <b>SNMP Commands . . . . .</b>               | <b>1057</b> |
|                    | Introduction . . . . .                       | 1057        |
|                    | alias (interface) . . . . .                  | 1059        |
|                    | debug snmp . . . . .                         | 1060        |
|                    | show counter snmp-server . . . . .           | 1061        |
|                    | show debugging snmp . . . . .                | 1065        |
|                    | show running-config snmp . . . . .           | 1066        |
|                    | show snmp-server . . . . .                   | 1067        |
|                    | show snmp-server community . . . . .         | 1068        |
|                    | show snmp-server group . . . . .             | 1069        |
|                    | show snmp-server user . . . . .              | 1070        |
|                    | show snmp-server view . . . . .              | 1071        |
|                    | snmp trap link-status . . . . .              | 1072        |
|                    | snmp trap link-status suppress . . . . .     | 1073        |
|                    | snmp-server . . . . .                        | 1075        |
|                    | snmp-server community . . . . .              | 1077        |
|                    | snmp-server contact . . . . .                | 1078        |
|                    | snmp-server enable trap . . . . .            | 1079        |
|                    | snmp-server engineID local . . . . .         | 1081        |
|                    | snmp-server engineID local reset . . . . .   | 1083        |
|                    | snmp-server group . . . . .                  | 1084        |
|                    | snmp-server host . . . . .                   | 1086        |
|                    | snmp-server legacy-ifadminstatus . . . . .   | 1088        |
|                    | snmp-server location . . . . .               | 1089        |
|                    | snmp-server source-interface . . . . .       | 1090        |
|                    | snmp-server startup-trap-delay . . . . .     | 1091        |
|                    | snmp-server user . . . . .                   | 1092        |
|                    | snmp-server view . . . . .                   | 1095        |
|                    | undebug snmp . . . . .                       | 1096        |
| <b>Chapter 24:</b> | <b>Mail (SMTP) Commands . . . . .</b>        | <b>1097</b> |
|                    | Introduction . . . . .                       | 1097        |
|                    | debug mail . . . . .                         | 1098        |
|                    | delete mail . . . . .                        | 1099        |
|                    | mail . . . . .                               | 1100        |
|                    | mail from . . . . .                          | 1102        |
|                    | mail smtpserver . . . . .                    | 1103        |
|                    | mail smtpserver authentication . . . . .     | 1104        |
|                    | mail smtpserver port . . . . .               | 1106        |
|                    | show counter mail . . . . .                  | 1108        |
|                    | show mail . . . . .                          | 1109        |
|                    | undebug mail . . . . .                       | 1110        |
| <b>Chapter 25:</b> | <b>Secure Shell (SSH) Commands . . . . .</b> | <b>1111</b> |

|                                      |      |
|--------------------------------------|------|
| Introduction                         | 1111 |
| banner login (SSH)                   | 1113 |
| clear ssh                            | 1114 |
| crypto key destroy hostkey           | 1115 |
| crypto key destroy userkey           | 1116 |
| crypto key generate hostkey          | 1117 |
| crypto key generate userkey          | 1119 |
| crypto key pubkey-chain userkey      | 1120 |
| debug ssh server                     | 1122 |
| service ssh                          | 1123 |
| show banner login                    | 1125 |
| show crypto key hostkey              | 1126 |
| show crypto key pubkey-chain userkey | 1128 |
| show crypto key userkey              | 1129 |
| show running-config ssh              | 1130 |
| show ssh                             | 1132 |
| show ssh server                      | 1134 |
| show ssh server allow-users          | 1136 |
| show ssh server deny-users           | 1137 |
| ssh server                           | 1138 |
| ssh server allow-users               | 1140 |
| ssh server authentication            | 1142 |
| ssh server deny-users                | 1144 |
| ssh server max-auth-tries            | 1146 |
| ssh server resolve-host              | 1147 |
| ssh server scp                       | 1148 |
| ssh server sftp                      | 1149 |
| undebg ssh server                    | 1150 |

**Chapter 26:**

|                             |             |
|-----------------------------|-------------|
| <b>Trigger Commands</b>     | <b>1151</b> |
| Introduction                | 1151        |
| active (trigger)            | 1153        |
| day                         | 1154        |
| debug trigger               | 1156        |
| description (trigger)       | 1157        |
| repeat                      | 1158        |
| script                      | 1159        |
| show debugging trigger      | 1161        |
| show running-config trigger | 1162        |
| show trigger                | 1163        |
| test                        | 1168        |
| time (trigger)              | 1169        |
| trap                        | 1171        |
| trigger                     | 1172        |
| trigger activate            | 1173        |
| type atmf node              | 1174        |
| type cpu                    | 1177        |
| type interface              | 1178        |
| type linkmon-probe          | 1179        |
| type log                    | 1181        |
| type memory                 | 1182        |
| type periodic               | 1183        |
| type ping-poll              | 1184        |

|                    |   |             |
|--------------------|---|-------------|
|                    | type reboot . . . . .   | 1185        |
|                    | type time . . . . .   | 1186        |
|                    | type usb . . . . .  | 1187        |
|                    | undebg trigger . . . . .  | 1188        |
| <b>Chapter 27:</b> | <b>Ping-Polling Commands . . . . .</b>                          | <b>1189</b> |
|                    | Introduction . . . . .  | 1189        |
|                    | active (ping-polling) . . . . .                                 | 1191        |
|                    | clear ping-poll . . . . .                                       | 1192        |
|                    | critical-interval . . . . .                                     | 1193        |
|                    | debug ping-poll . . . . .                                       | 1194        |
|                    | description (ping-polling) . . . . .                            | 1195        |
|                    | fail-count . . . . .  | 1196        |
|                    | ip (ping-polling) . . . . .                                     | 1197        |
|                    | length (ping-poll data) . . . . .                               | 1198        |
|                    | normal-interval . . . . .                                       | 1199        |
|                    | ping-poll . . . . .   | 1200        |
|                    | sample-size . . . . .   | 1201        |
|                    | show counter ping-poll . . . . .                                | 1203        |
|                    | show ping-poll . . . . .  | 1205        |
|                    | source-ip . . . . .   | 1209        |
|                    | timeout (ping polling) . . . . .                                | 1211        |
|                    | up-count . . . . .  | 1212        |
|                    | undebg ping-poll . . . . .                                      | 1213        |
| <b>PART 6:</b>     | <b>Firewall and Network Address Translation (NAT) . . . . .</b> | <b>1214</b> |
| <b>Chapter 28:</b> | <b>Firewall Commands . . . . .</b>                              | <b>1215</b> |
|                    | Introduction . . . . .  | 1215        |
|                    | clear firewall connections . . . . .                            | 1217        |
|                    | connection-limit (firewall) . . . . .                           | 1218        |
|                    | connection-log events . . . . .                                 | 1219        |
|                    | firewall . . . . .  | 1220        |
|                    | debug firewall . . . . .  | 1221        |
|                    | ip tcp timeout established . . . . .                            | 1222        |
|                    | move rule (firewall) . . . . .                                  | 1223        |
|                    | protect (firewall) . . . . .                                    | 1224        |
|                    | rule (firewall) . . . . .                                       | 1225        |
|                    | show connection-log events . . . . .                            | 1227        |
|                    | show firewall . . . . .   | 1228        |
|                    | show firewall connections . . . . .                             | 1229        |
|                    | show firewall connections limits . . . . .                      | 1230        |
|                    | show firewall connections limits config-check . . . . .         | 1231        |
|                    | show firewall rule . . . . .                                    | 1232        |
|                    | show firewall rule config-check . . . . .                       | 1234        |
|                    | show debugging firewall . . . . .                               | 1235        |
|                    | show running-config firewall . . . . .                          | 1236        |
| <b>Chapter 29:</b> | <b>Application and Entity Commands . . . . .</b>                | <b>1237</b> |
|                    | Introduction . . . . .  | 1237        |
|                    | application . . . . .   | 1239        |
|                    | dport . . . . .   | 1241        |

|                    |  |             |
|--------------------|--|-------------|
|                    | dscp . . . . .                                   | 1243        |
|                    | host (network) . . . . .                         | 1245        |
|                    | icmp-code . . . . .                              | 1247        |
|                    | icmp-type . . . . .                              | 1249        |
|                    | ip address (host) . . . . .                      | 1251        |
|                    | ip subnet . . . . .                              | 1253        |
|                    | ipv6 address (host) . . . . .                    | 1255        |
|                    | ipv6 subnet . . . . .                            | 1257        |
|                    | network (zone) . . . . .                         | 1259        |
|                    | protocol . . . . .                               | 1261        |
|                    | show application . . . . .                       | 1262        |
|                    | show application detail . . . . .                | 1263        |
|                    | show entity . . . . .                            | 1264        |
|                    | sport . . . . .                                  | 1267        |
|                    | zone . . . . .                                   | 1269        |
| <b>Chapter 30:</b> | <b>NAT Commands . . . . .</b>                    | <b>1271</b> |
|                    | Introduction . . . . .                           | 1271        |
|                    | enable (nat) . . . . .                           | 1273        |
|                    | ip limited-local-proxy-arp . . . . .             | 1274        |
|                    | local-proxy-arp . . . . .                        | 1276        |
|                    | move rule (nat) . . . . .                        | 1277        |
|                    | nat . . . . .                                    | 1278        |
|                    | rule (nat) . . . . .                             | 1279        |
|                    | show nat . . . . .                               | 1283        |
|                    | show nat rule . . . . .                          | 1284        |
|                    | show nat rule config-check . . . . .             | 1286        |
|                    | show running-config nat . . . . .                | 1287        |
| <b>PART 7:</b>     | <b>Advanced Network Protection . . . . .</b>     | <b>1288</b> |
| <b>Chapter 31:</b> | <b>IPS Commands . . . . .</b>                    | <b>1289</b> |
|                    | Introduction . . . . .                           | 1289        |
|                    | category action (IPS) . . . . .                  | 1290        |
|                    | ips . . . . .                                    | 1291        |
|                    | protect (IPS) . . . . .                          | 1292        |
|                    | show ips . . . . .                               | 1293        |
|                    | show ips categories . . . . .                    | 1294        |
|                    | show running-config ips . . . . .                | 1296        |
| <b>Chapter 32:</b> | <b>URL Filtering Commands . . . . .</b>          | <b>1297</b> |
|                    | Introduction . . . . .                           | 1297        |
|                    | blacklist . . . . .                              | 1299        |
|                    | log url-requests . . . . .                       | 1300        |
|                    | protect (url-filter) . . . . .                   | 1301        |
|                    | show running-config url-filter . . . . .         | 1302        |
|                    | show url-filter . . . . .                        | 1303        |
|                    | url-filter reload custom-lists . . . . .         | 1304        |
|                    | url-filter . . . . .                             | 1305        |
|                    | whitelist (url-filter) . . . . .                 | 1306        |
| <b>PART 8:</b>     | <b>Virtual Private Networks (VPNs) . . . . .</b> | <b>1307</b> |

|                    |  |             |
|--------------------|--|-------------|
| <b>Chapter 33:</b> | <b>IPsec Commands</b> . . . . .                      | <b>1308</b> |
|                    | Introduction . . . . .                               | 1308        |
|                    | clear isakmp sa . . . . .                            | 1310        |
|                    | crypto ipsec profile . . . . .                       | 1311        |
|                    | crypto isakmp key . . . . .                          | 1313        |
|                    | crypto isakmp peer . . . . .                         | 1316        |
|                    | crypto isakmp profile . . . . .                      | 1318        |
|                    | debug isakmp . . . . .                               | 1320        |
|                    | dpd-interval . . . . .                               | 1322        |
|                    | dpd-timeout . . . . .                                | 1323        |
|                    | interface tunnel (IPsec) . . . . .                   | 1324        |
|                    | lifetime (IPsec Profile) . . . . .                   | 1325        |
|                    | lifetime (ISAKMP Profile) . . . . .                  | 1326        |
|                    | no debug isakmp . . . . .                            | 1327        |
|                    | pfs . . . . .  | 1328        |
|                    | rekey . . . . .                                      | 1330        |
|                    | show debugging isakmp . . . . .                      | 1331        |
|                    | show interface tunnel (IPsec) . . . . .              | 1332        |
|                    | show ipsec counters . . . . .                        | 1333        |
|                    | show ipsec peer . . . . .                            | 1334        |
|                    | show ipsec policy . . . . .                          | 1335        |
|                    | show ipsec profile . . . . .                         | 1336        |
|                    | show ipsec sa . . . . .                              | 1338        |
|                    | show isakmp counters . . . . .                       | 1339        |
|                    | show isakmp key (IPsec) . . . . .                    | 1340        |
|                    | show isakmp peer . . . . .                           | 1341        |
|                    | show isakmp profile . . . . .                        | 1342        |
|                    | show isakmp sa . . . . .                             | 1344        |
|                    | transform (IPsec Profile) . . . . .                  | 1345        |
|                    | transform (ISAKMP Profile) . . . . .                 | 1346        |
|                    | tunnel destination (IPsec) . . . . .                 | 1348        |
|                    | tunnel local name (IPsec) . . . . .                  | 1350        |
|                    | tunnel local selector . . . . .                      | 1351        |
|                    | tunnel mode ipsec . . . . .                          | 1353        |
|                    | tunnel protection ipsec (IPsec) . . . . .            | 1354        |
|                    | tunnel remote name (IPsec) . . . . .                 | 1355        |
|                    | tunnel remote selector . . . . .                     | 1356        |
|                    | tunnel security-reprocessing . . . . .               | 1358        |
|                    | tunnel selector paired . . . . .                     | 1359        |
|                    | tunnel source (IPsec) . . . . .                      | 1360        |
|                    | undebg isakmp . . . . .                              | 1362        |
|                    | version (ISAKMP) . . . . .                           | 1363        |
| <br>               |  |             |
| <b>Chapter 34:</b> | <b>Transitioning IPv4 to IPv6 Commands</b> . . . . . | <b>1364</b> |
|                    | Introduction . . . . .                               | 1364        |
|                    | br-address (software) . . . . .                      | 1366        |
|                    | mesh-mode . . . . .                                  | 1367        |
|                    | method (software) . . . . .                          | 1368        |
|                    | rule (software) . . . . .                            | 1369        |
|                    | show running-config software-configuration . . . . . | 1371        |
|                    | show software-configuration . . . . .                | 1372        |
|                    | software-configuration . . . . .                     | 1374        |

|  |      |
|--|------|
| tunnel security-reprocessing . . . . . | 1375 |
| tunnel destination (DS-Lite) . . . . . | 1376 |
| tunnel mode ds-lite . . . . .          | 1377 |
| tunnel mode lw4o6 . . . . .            | 1378 |
| tunnel mode map-e . . . . .            | 1379 |
| tunnel software . . . . .              | 1380 |
| upstream-interface . . . . .           | 1381 |

**Chapter 35: IPv6 Tunneling Commands . . . . . 1382**

|   |      |
|---|------|
| Introduction . . . . .                            | 1382 |
| interface tunnel (IPv6) . . . . .                 | 1383 |
| ip address (IP Addressing and Protocol) . . . . . | 1384 |
| ip tcp adjust-mss . . . . .                       | 1385 |
| ipv6 address . . . . .                            | 1387 |
| ipv6 tcp adjust-mss . . . . .                     | 1389 |
| mtu . . . . .                                     | 1391 |
| show interface tunnel (IPv6) . . . . .            | 1393 |
| tunnel destination (IPv6) . . . . .               | 1394 |
| tunnel dscp . . . . .                             | 1396 |
| tunnel mode (IPv6) . . . . .                      | 1397 |
| tunnel source (IPv6) . . . . .                    | 1398 |
| tunnel ttl . . . . .                              | 1400 |

# List of Commands

|  |      |
|--|------|
| aaa authentication enable default local .....          | 114  |
| aaa local authentication attempts lockout-time .....   | 115  |
| aaa local authentication attempts max-fail .....       | 116  |
| aaa login fail-delay .....                             | 117  |
| accept-invalid-sslcert .....                           | 520  |
| activate .....   | 325  |
| active (ping-polling) .....                            | 1191 |
| active (trigger) .....                                 | 1153 |
| address prefix .....                                   | 970  |
| address range .....                                    | 972  |
| ageing-time .....                                      | 398  |
| alias (interface) .....                                | 1059 |
| apn .....  | 351  |
| application .....                                      | 1239 |
| application-proxy ip-filter .....                      | 653  |
| application-proxy quarantine-vlan .....                | 654  |
| application-proxy redirect-url .....                   | 655  |
| application-proxy threat-protection send-summary ..... | 657  |
| application-proxy threat-protection .....              | 656  |
| application-proxy whitelist enable .....               | 658  |
| application-proxy whitelist server .....               | 659  |
| area-link .....  | 661  |
| arp log .....  | 477  |
| arp opportunistic-nd .....                             | 480  |
| arp .....  | 476  |

---

|   |     |
|---|-----|
| arp-aging-timeout.....                    | 475 |
| arp-reply-bc-dmac.....                    | 481 |
| atmf area password.....                   | 665 |
| atmf area.....                            | 663 |
| atmf authorize provision.....             | 669 |
| atmf authorize.....                       | 667 |
| atmf backup area-masters delete.....      | 672 |
| atmf backup area-masters enable.....      | 673 |
| atmf backup area-masters now.....         | 674 |
| atmf backup area-masters synchronize..... | 675 |
| atmf backup bandwidth.....                | 676 |
| atmf backup delete.....                   | 677 |
| atmf backup enable.....                   | 678 |
| atmf backup guests delete.....            | 679 |
| atmf backup guests enable.....            | 680 |
| atmf backup guests now.....               | 681 |
| atmf backup guests synchronize.....       | 682 |
| atmf backup now.....                      | 683 |
| atmf backup redundancy enable.....        | 685 |
| atmf backup server.....                   | 686 |
| atmf backup stop.....                     | 688 |
| atmf backup synchronize.....              | 689 |
| atmf backup.....                          | 671 |
| atmf cleanup.....                         | 690 |
| atmf container login.....                 | 692 |
| atmf container.....                       | 691 |
| atmf controller.....                      | 693 |
| atmf distribute firmware.....             | 694 |
| atmf domain vlan.....                     | 696 |
| atmf enable.....                          | 699 |
| atmf group (membership).....              | 700 |
| atmf guest-class.....                     | 702 |
| atmf log-verbose.....                     | 704 |
| atmf management subnet.....               | 705 |
| atmf management vlan.....                 | 708 |



---

|   |      |
|---|------|
| atmf master .....                         | 710  |
| atmf mtu .....                            | 711  |
| atmf network-name .....                   | 712  |
| atmf provision (interface) .....          | 713  |
| atmf provision node .....                 | 714  |
| atmf reboot-rolling .....                 | 716  |
| atmf recover guest .....                  | 722  |
| atmf recover led-off .....                | 723  |
| atmf recover .....                        | 720  |
| atmf recovery-server .....                | 724  |
| atmf remote-login .....                   | 726  |
| atmf restricted-login .....               | 728  |
| atmf secure-mode certificate expire ..... | 732  |
| atmf secure-mode certificate expiry ..... | 733  |
| atmf secure-mode certificate renew .....  | 734  |
| atmf secure-mode enable-all .....         | 735  |
| atmf secure-mode .....                    | 730  |
| atmf select-area .....                    | 737  |
| atmf topology-gui enable .....            | 158  |
| atmf topology-gui enable .....            | 738  |
| atmf trustpoint .....                     | 739  |
| atmf virtual-crosslink .....              | 741  |
| atmf virtual-link protection .....        | 746  |
| atmf virtual-link .....                   | 743  |
| atmf working-set .....                    | 748  |
| autoboot enable .....                     | 64   |
| backpressure .....                        | 366  |
| banner exec .....                         | 171  |
| banner login (SSH) .....                  | 1113 |
| banner login (system) .....               | 173  |
| banner motd .....                         | 175  |
| blacklist .....                           | 1299 |
| boot config-file backup .....             | 67   |
| boot config-file .....                    | 65   |
| boot system backup .....                  | 69   |

---

|   |      |
|---|------|
| boot system .....                               | 68   |
| bootfile .....                                  | 901  |
| br-address (software) .....                     | 1366 |
| bridge .....                                    | 399  |
| bridge-group .....                              | 400  |
| bridge-group .....                              | 750  |
| category action (IPS) .....                     | 1290 |
| cd .....  | 70   |
| chat-script .....                               | 353  |
| cid .....                                       | 354  |
| clear aaa local user lockout .....              | 118  |
| clear application-proxy threat-protection ..... | 751  |
| clear arp-cache .....                           | 482  |
| clear atmf links statistics .....               | 754  |
| clear atmf links virtual .....                  | 753  |
| clear atmf links .....                          | 752  |
| clear atmf recovery-file .....                  | 755  |
| clear atmf secure-mode certificates .....       | 756  |
| clear atmf secure-mode statistics .....         | 757  |
| clear counter ipv6 dhcp-client .....            | 974  |
| clear counter ipv6 dhcp-server .....            | 975  |
| clear exception log .....                       | 230  |
| clear firewall connections .....                | 1217 |
| clear ip dhcp binding .....                     | 902  |
| clear ip dns forwarding cache .....             | 521  |
| clear ipv6 dhcp binding .....                   | 976  |
| clear ipv6 dhcp client .....                    | 978  |
| clear ipv6 neighbors .....                      | 571  |
| clear isakmp sa .....                           | 1310 |
| clear line console .....                        | 119  |
| clear line vty .....                            | 120  |
| clear log buffered .....                        | 232  |
| clear log external .....                        | 233  |
| clear log permanent .....                       | 234  |
| clear log .....                                 | 231  |

---

|  |      |
|--|------|
| clear mac address-table dynamic.....       | 368  |
| clear mac address-table static.....        | 369  |
| clear mac-filter counter.....              | 401  |
| clear ping-poll.....                       | 1192 |
| clear port counter.....                    | 370  |
| clear ssh.....                             | 1114 |
| clock set.....                             | 177  |
| clock summer-time date.....                | 178  |
| clock summer-time recurring.....           | 180  |
| clock timezone.....                        | 182  |
| clone (amf-provision).....                 | 758  |
| configure boot config (amf-provision)..... | 760  |
| configure boot system (amf-provision)..... | 762  |
| configure terminal.....                    | 51   |
| connection-limit (firewall).....           | 1218 |
| connection-log events.....                 | 1219 |
| connection-log events.....                 | 235  |
| copy (amf-provision).....                  | 764  |
| copy (filename).....                       | 71   |
| copy buffered-log.....                     | 236  |
| copy current-software.....                 | 73   |
| copy debug.....                            | 74   |
| copy permanent-log.....                    | 237  |
| copy running-config.....                   | 75   |
| copy startup-config.....                   | 76   |
| copy zmodem.....                           | 77   |
| create (amf-provision).....                | 765  |
| create autoboot.....                       | 78   |
| critical-interval.....                     | 1193 |
| crypto ipsec profile.....                  | 1311 |
| crypto isakmp key.....                     | 1313 |
| crypto isakmp peer.....                    | 1316 |
| crypto isakmp profile.....                 | 1318 |
| crypto key destroy hostkey.....            | 1115 |
| crypto key destroy userkey.....            | 1116 |

---

|                                       |      |
|---------------------------------------|------|
| crypto key generate hostkey .....     | 1117 |
| crypto key generate rsa .....         | 626  |
| crypto key generate userkey .....     | 1119 |
| crypto key pubkey-chain userkey ..... | 1120 |
| crypto key zeroize .....              | 627  |
| crypto pki authenticate .....         | 628  |
| crypto pki enroll .....               | 629  |
| crypto pki export pem .....           | 630  |
| crypto pki export pkcs12 .....        | 631  |
| crypto pki import pem .....           | 632  |
| crypto pki import pkcs12 .....        | 634  |
| crypto pki trustpoint .....           | 635  |
| day .....                             | 1154 |
| ddns enable .....                     | 522  |
| ddns-update now .....                 | 524  |
| ddns-update-method .....              | 523  |
| debug atmf packet .....               | 769  |
| debug atmf .....                      | 767  |
| debug core-file .....                 | 183  |
| debug ddns .....                      | 525  |
| debug firewall .....                  | 1221 |
| debug ip dns forwarding .....         | 526  |
| debug ip packet interface .....       | 483  |
| debug isakmp .....                    | 1320 |
| debug mail .....                      | 1098 |
| debug ping-poll .....                 | 1194 |
| debug platform packet .....           | 371  |
| debug ppp .....                       | 431  |
| debug snmp .....                      | 1060 |
| debug ssh server .....                | 1122 |
| debug trigger .....                   | 1156 |
| default log buffered .....            | 238  |
| default log console .....             | 239  |
| default log email .....               | 240  |
| default log external .....            | 241  |

---

|                                     |      |
|-------------------------------------|------|
| default log host.....               | 242  |
| default log monitor.....            | 243  |
| default log permanent.....          | 244  |
| default-action.....                 | 402  |
| default-protocol-action.....        | 404  |
| default-router.....                 | 903  |
| delete (amf-provision).....         | 772  |
| delete debug.....                   | 80   |
| delete mail.....                    | 1099 |
| delete.....                         | 79   |
| description (amf-container).....    | 776  |
| description (Domain List).....      | 527  |
| description (interface).....        | 329  |
| description (ping-polling).....     | 1195 |
| description (trigger).....          | 1157 |
| dir.....                            | 81   |
| disable (Privileged Exec mode)..... | 52   |
| discovery.....                      | 774  |
| dns-server (DHCPv6).....            | 979  |
| dns-server.....                     | 904  |
| do.....                             | 53   |
| domain (Domain List).....           | 528  |
| domain-name (DHCPv6).....           | 981  |
| domain-name.....                    | 905  |
| dpd-interval.....                   | 1322 |
| dpd-timeout.....                    | 1323 |
| dport.....                          | 1241 |
| dscp.....                           | 1243 |
| duplex.....                         | 373  |
| echo.....                           | 326  |
| edit (filename).....                | 84   |
| edit.....                           | 83   |
| enable (nat).....                   | 1273 |
| enable (Privileged Exec mode).....  | 54   |
| enable password.....                | 121  |

---

|   |      |
|---|------|
| enable secret .....                           | 124  |
| encapsulation ppp .....                       | 355  |
| encapsulation ppp .....                       | 434  |
| end .....                                     | 56   |
| enrollment (ca-trustpoint) .....              | 636  |
| erase factory-default .....                   | 777  |
| erase factory-default .....                   | 85   |
| erase startup-config .....                    | 86   |
| exec-timeout .....                            | 127  |
| exit .....                                    | 57   |
| fail-count .....                              | 1196 |
| fingerprint (ca-trustpoint) .....             | 637  |
| firewall .....                                | 1220 |
| flowcontrol (switch port) .....               | 374  |
| flowcontrol hardware (asyn/console) .....     | 129  |
| help .....                                    | 58   |
| host (DHCP) .....                             | 906  |
| host (network) .....                          | 1245 |
| host-name (DDNS) .....                        | 529  |
| hostname .....                                | 184  |
| http port .....                               | 159  |
| http secure-port .....                        | 160  |
| http-enable .....                             | 778  |
| icmp-code .....                               | 1247 |
| icmp-type .....                               | 1249 |
| identity (amf-provision) .....                | 780  |
| interface (PPP) .....                         | 435  |
| interface (to configure) .....                | 330  |
| interface tunnel (IPsec) .....                | 1324 |
| interface tunnel (IPv6) .....                 | 1383 |
| ip (ping-polling) .....                       | 1197 |
| ip address (host) .....                       | 1251 |
| ip address (IP Addressing and Protocol) ..... | 1384 |
| ip address (IP Addressing and Protocol) ..... | 485  |
| ip address dhcp .....                         | 907  |

---

|  |     |
|--|-----|
| ip address negotiated.....                               | 436 |
| ip ddns-update-method .....                              | 530 |
| ip dhcp bootp ignore .....                               | 909 |
| ip dhcp leasequery enable .....                          | 910 |
| ip dhcp option.....                                      | 911 |
| ip dhcp pool.....  | 913 |
| ip dhcp-client default-route distance .....              | 914 |
| ip dhcp-client request vendor-identifying-specific ..... | 916 |
| ip dhcp-client vendor-identifying-class .....            | 917 |
| ip dhcp-relay agent-option checking .....                | 920 |
| ip dhcp-relay agent-option checking .....                | 984 |
| ip dhcp-relay agent-option remote-id .....               | 922 |
| ip dhcp-relay agent-option remote-id .....               | 986 |
| ip dhcp-relay agent-option .....                         | 918 |
| ip dhcp-relay agent-option .....                         | 982 |
| ip dhcp-relay information policy .....                   | 924 |
| ip dhcp-relay information policy .....                   | 988 |
| ip dhcp-relay maxhops .....                              | 926 |
| ip dhcp-relay maxhops .....                              | 990 |
| ip dhcp-relay max-message-length.....                    | 927 |
| ip dhcp-relay max-message-length.....                    | 991 |
| ip dhcp-relay server-address .....                       | 929 |
| ip dhcp-relay server-address .....                       | 993 |
| ip dhcp-relay use-client-side-address.....               | 931 |
| ip directed-broadcast.....                               | 486 |
| ip dns forwarding cache .....                            | 532 |
| ip dns forwarding dead-time.....                         | 533 |
| ip dns forwarding domain-list .....                      | 534 |
| ip dns forwarding retry .....                            | 535 |
| ip dns forwarding source-interface .....                 | 536 |
| ip dns forwarding timeout .....                          | 537 |
| ip dns forwarding.....                                   | 531 |
| ip domain-list.....                                      | 538 |
| ip domain-lookup .....                                   | 539 |
| ip domain-name.....                                      | 541 |

---

|                                      |      |
|--------------------------------------|------|
| ip forward-protocol udp .....        | 488  |
| ip gratuitous-arp-link .....         | 490  |
| ip helper-address .....              | 492  |
| ip limited-local-proxy-arp .....     | 1274 |
| ip limited-local-proxy-arp .....     | 494  |
| ip local-proxy-arp .....             | 496  |
| ip name-server preferred-order ..... | 544  |
| ip name-server .....                 | 542  |
| ip proxy-arp .....                   | 497  |
| ip redirects .....                   | 498  |
| ip route .....                       | 612  |
| ip subnet .....                      | 1253 |
| ip tcp adjust-mss .....              | 1385 |
| ip tcp adjust-mss .....              | 332  |
| ip tcp adjust-mss .....              | 438  |
| ip tcp synack-retries .....          | 499  |
| ip tcp timeout established .....     | 1222 |
| ip tcp timeout established .....     | 500  |
| ip tftp source-interface .....       | 87   |
| ip unnumbered .....                  | 440  |
| ip unreachable .....                 | 501  |
| ips .....                            | 1291 |
| ipv6 address (DHCPv6 PD) .....       | 995  |
| ipv6 address (host) .....            | 1255 |
| ipv6 address autoconfig .....        | 574  |
| ipv6 address dhcp .....              | 998  |
| ipv6 address suffix .....            | 576  |
| ipv6 address .....                   | 1387 |
| ipv6 address .....                   | 572  |
| ipv6 ddns-update-method .....        | 545  |
| ipv6 dhcp client pd .....            | 1000 |
| ipv6 dhcp option .....               | 1002 |
| ipv6 dhcp pool .....                 | 1004 |
| ipv6 dhcp server .....               | 1006 |
| ipv6 enable .....                    | 577  |



---

|                                    |      |
|------------------------------------|------|
| ipv6 eui64-linklocal .....         | 579  |
| ipv6 forwarding .....              | 580  |
| ipv6 local pool .....              | 1007 |
| ipv6 nd accept-ra-pinfo .....      | 581  |
| ipv6 nd current-hoplimit .....     | 582  |
| ipv6 nd managed-config-flag .....  | 584  |
| ipv6 nd minimum-ra-interval .....  | 585  |
| ipv6 nd other-config-flag .....    | 587  |
| ipv6 nd prefix (DHCPv6) .....      | 1009 |
| ipv6 nd prefix .....               | 588  |
| ipv6 nd proxy interface .....      | 590  |
| ipv6 nd ra-interval .....          | 591  |
| ipv6 nd ra-lifetime .....          | 592  |
| ipv6 nd reachable-time .....       | 593  |
| ipv6 nd retransmission-time .....  | 595  |
| ipv6 nd suppress-ra .....          | 597  |
| ipv6 neighbor .....                | 598  |
| ipv6 opportunistic-nd .....        | 599  |
| ipv6 route .....                   | 600  |
| ipv6 route .....                   | 614  |
| ipv6 subnet .....                  | 1257 |
| ipv6 tcp adjust-mss .....          | 1389 |
| ipv6 tcp adjust-mss .....          | 334  |
| ipv6 tcp adjust-mss .....          | 442  |
| ipv6 tftp source-interface .....   | 88   |
| ipv6 unreachable .....             | 601  |
| keepalive (PPP) .....              | 444  |
| l3-filtering enable .....          | 405  |
| lease .....                        | 933  |
| length (asyn) .....                | 131  |
| length (ping-poll data) .....      | 1198 |
| license-cert (amf-provision) ..... | 782  |
| lifetime (IPsec Profile) .....     | 1325 |
| lifetime (ISAKMP Profile) .....    | 1326 |
| line .....                         | 132  |

---

|                              |      |
|------------------------------|------|
| link-address .....           | 1011 |
| linkflap action .....        | 376  |
| local-proxy-arp .....        | 1276 |
| local-proxy-arp .....        | 503  |
| locate (amf-provision) ..... | 784  |
| log buffered (filter) .....  | 246  |
| log buffered exclude.....    | 249  |
| log buffered size.....       | 252  |
| log buffered .....           | 245  |
| log console (filter) .....   | 254  |
| log console exclude .....    | 257  |
| log console.....             | 253  |
| log date-format.....         | 260  |
| log email (filter).....      | 262  |
| log email exclude.....       | 265  |
| log email time .....         | 268  |
| log email .....              | 261  |
| log event-host.....          | 161  |
| log event-host.....          | 786  |
| log external (filter) .....  | 272  |
| log external exclude .....   | 275  |
| log external rotate.....     | 278  |
| log external size .....      | 280  |
| log external .....           | 270  |
| log facility .....           | 281  |
| log host (filter).....       | 285  |
| log host exclude .....       | 288  |
| log host source .....        | 291  |
| log host startup-delay ..... | 292  |
| log host time .....          | 294  |
| log host .....               | 283  |
| log monitor (filter) .....   | 296  |
| log monitor exclude .....    | 299  |
| log permanent (filter) ..... | 303  |
| log permanent exclude .....  | 306  |

---

|                                      |      |
|--------------------------------------|------|
| log permanent size .....             | 309  |
| log permanent .....                  | 302  |
| log trustpoint.....                  | 311  |
| log url-requests.....                | 1300 |
| log url-requests.....                | 312  |
| logout.....                          | 59   |
| log-rate-limit nsm .....             | 310  |
| mac address-table acquire .....      | 377  |
| mac address-table ageing-time .....  | 378  |
| mac address-table static .....       | 379  |
| mac-filter.....                      | 407  |
| mac-filter-group egress.....         | 406  |
| mac-filter-group.....                | 408  |
| mac-learning .....                   | 409  |
| mail from.....                       | 1102 |
| mail smtpserver authentication ..... | 1104 |
| mail smtpserver port.....            | 1106 |
| mail smtpserver .....                | 1103 |
| mail .....                           | 1100 |
| max-fib-routes.....                  | 186  |
| max-fib-routes.....                  | 615  |
| maximum-paths.....                   | 617  |
| max-static-routes.....               | 187  |
| max-static-routes.....               | 616  |
| mesh-mode .....                      | 1367 |
| method (software) .....              | 1368 |
| mkdir .....                          | 89   |
| modeltype .....                      | 787  |
| move debug.....                      | 91   |
| move rule (firewall) .....           | 1223 |
| move rule (nat) .....                | 1277 |
| move.....                            | 90   |
| mru jumbo .....                      | 336  |
| mtu (PPP) .....                      | 446  |
| mtu .....                            | 1391 |

---

|                                    |      |
|------------------------------------|------|
| mtu .....                          | 337  |
| nat .....                          | 1278 |
| network (DHCP) .....               | 935  |
| network (zone) .....               | 1259 |
| next-server .....                  | 936  |
| no crypto pki certificate .....    | 639  |
| no debug all .....                 | 188  |
| no debug isakmp .....              | 1327 |
| normal-interval .....              | 1199 |
| ntp authenticate .....             | 1036 |
| ntp authentication-key .....       | 1037 |
| ntp broadcastdelay .....           | 1038 |
| ntp discard .....                  | 1039 |
| ntp master .....                   | 1040 |
| ntp peer .....                     | 1041 |
| ntp rate-limit .....               | 1043 |
| ntp restrict .....                 | 1044 |
| ntp server .....                   | 1046 |
| ntp source .....                   | 1048 |
| ntp trusted-key (deprecated) ..... | 1050 |
| optimistic-nd .....                | 504  |
| optimistic-nd .....                | 602  |
| option (DHCPv6) .....              | 1013 |
| option .....                       | 937  |
| password (DDNS) .....              | 546  |
| peer default ip address .....      | 447  |
| peer neighbor-route .....          | 449  |
| pfs .....                          | 1328 |
| ping ipv6 .....                    | 603  |
| ping .....                         | 505  |
| ping-poll .....                    | 1200 |
| polarity .....                     | 380  |
| ppp authentication refuse .....    | 453  |
| ppp authentication .....           | 451  |
| ppp hostname .....                 | 455  |

---

|                                   |      |
|-----------------------------------|------|
| ppp ipcp dns suffix-list.....     | 459  |
| ppp ipcp dns suffix-list.....     | 549  |
| ppp ipcp dns .....                | 457  |
| ppp ipcp dns .....                | 547  |
| ppp ipcp ip-override .....        | 461  |
| ppp password .....                | 462  |
| ppp service-name (PPPoE) .....    | 463  |
| ppp timeout idle.....             | 464  |
| ppp username.....                 | 465  |
| prefix-delegation pool.....       | 1015 |
| privilege level .....             | 134  |
| probe enable .....                | 939  |
| probe packets .....               | 940  |
| probe timeout.....                | 941  |
| probe type .....                  | 942  |
| protect (firewall).....           | 1224 |
| protect (IPS) .....               | 1292 |
| protect (url-filter) .....        | 1301 |
| protocol ethii (macfilter) .....  | 410  |
| protocol novell (macfilter) ..... | 412  |
| protocol sap (macfilter) .....    | 414  |
| protocol snap (macfilter).....    | 416  |
| protocol.....                     | 1261 |
| pwd.....                          | 92   |
| range .....                       | 943  |
| reboot .....                      | 190  |
| receive-packet-scheduler .....    | 191  |
| rekey.....                        | 1330 |
| reload.....                       | 193  |
| repeat.....                       | 1158 |
| retry-interval (DDNS).....        | 551  |
| rmdir.....                        | 93   |
| route.....                        | 944  |
| rsakeypair (ca-trustpoint) .....  | 640  |
| rule (firewall) .....             | 1225 |

---

|  |      |
|--|------|
| rule (macfilter).....                            | 418  |
| rule (nat).....                                  | 1279 |
| rule (softwire).....                             | 1369 |
| rule ip (macfilter).....                         | 420  |
| rule ipv6 (macfilter).....                       | 422  |
| sample-size.....                                 | 1201 |
| script.....                                      | 1159 |
| security-password forced-change.....             | 136  |
| security-password history.....                   | 135  |
| security-password lifetime.....                  | 137  |
| security-password minimum-categories.....        | 139  |
| security-password minimum-length.....            | 140  |
| security-password min-lifetime-enforce.....      | 138  |
| security-password reject-expired-pwd.....        | 141  |
| security-password warning.....                   | 142  |
| service advanced-vty.....                        | 143  |
| service atmf-application-proxy.....              | 788  |
| service dhcp-relay.....                          | 1017 |
| service dhcp-relay.....                          | 945  |
| service dhcp-server.....                         | 946  |
| service http.....                                | 162  |
| service password-encryption.....                 | 144  |
| service ssh.....                                 | 1123 |
| service statistics interfaces counter.....       | 339  |
| service telnet.....                              | 145  |
| short-lease-threshold.....                       | 947  |
| show aaa local user locked.....                  | 146  |
| show application detail.....                     | 1263 |
| show application.....                            | 1262 |
| show application-proxy threat-protection.....    | 789  |
| show application-proxy whitelist interface.....  | 791  |
| show application-proxy whitelist server.....     | 793  |
| show application-proxy whitelist supplicant..... | 794  |
| show arp.....                                    | 506  |
| show atmf area guests.....                       | 803  |

---

|   |      |
|---|------|
| show atmf area guests-detail.....       | 805  |
| show atmf area nodes .....              | 807  |
| show atmf area nodes-detail .....       | 809  |
| show atmf area summary .....            | 811  |
| show atmf area .....                    | 800  |
| show atmf authorization .....           | 812  |
| show atmf backup area .....             | 819  |
| show atmf backup guest.....             | 821  |
| show atmf backup.....                   | 815  |
| show atmf container.....                | 823  |
| show atmf detail.....                   | 826  |
| show atmf group members .....           | 830  |
| show atmf group .....                   | 828  |
| show atmf guests detail.....            | 834  |
| show atmf guests.....                   | 832  |
| show atmf links detail.....             | 839  |
| show atmf links guest detail.....       | 850  |
| show atmf links guest.....              | 848  |
| show atmf links statistics.....         | 854  |
| show atmf links.....                    | 837  |
| show atmf nodes .....                   | 857  |
| show atmf provision nodes .....         | 859  |
| show atmf recovery-file.....            | 861  |
| show atmf secure-mode audit link .....  | 865  |
| show atmf secure-mode audit .....       | 864  |
| show atmf secure-mode certificates..... | 866  |
| show atmf secure-mode sa.....           | 869  |
| show atmf secure-mode statistics .....  | 872  |
| show atmf secure-mode .....             | 862  |
| show atmf tech.....                     | 874  |
| show atmf virtual-links.....            | 877  |
| show atmf working-set .....             | 879  |
| show atmf.....                          | 796  |
| show autoboot .....                     | 94   |
| show banner login.....                  | 1125 |

---

|   |      |
|---|------|
| show boot.....                            | 95   |
| show bridge macaddr .....                 | 426  |
| show bridge.....                          | 424  |
| show cellular .....                       | 356  |
| show clock .....                          | 194  |
| show connection-log events .....          | 1227 |
| show connection-log events .....          | 313  |
| show counter dhcp-client.....             | 949  |
| show counter dhcp-relay .....             | 1018 |
| show counter dhcp-relay .....             | 950  |
| show counter dhcp-server .....            | 953  |
| show counter ipv6 dhcp-client.....        | 1021 |
| show counter ipv6 dhcp-server .....       | 1023 |
| show counter log.....                     | 314  |
| show counter mail.....                    | 1108 |
| show counter ntp (deprecated) .....       | 1051 |
| show counter ping-poll.....               | 1203 |
| show counter snmp-server.....             | 1061 |
| show cpu history .....                    | 199  |
| show cpu.....                             | 196  |
| show crypto key hostkey.....              | 1126 |
| show crypto key mypubkey rsa.....         | 641  |
| show crypto key pubkey-chain userkey..... | 1128 |
| show crypto key userkey.....              | 1129 |
| show crypto pki certificates .....        | 642  |
| show crypto pki trustpoint .....          | 644  |
| show ddns-update-method status .....      | 552  |
| show debugging atmf packet .....          | 881  |
| show debugging atmf .....                 | 880  |
| show debugging firewall.....              | 1235 |
| show debugging ip dns forwarding .....    | 553  |
| show debugging ip packet.....             | 507  |
| show debugging isakmp.....                | 1331 |
| show debugging platform packet .....      | 381  |
| show debugging ppp.....                   | 466  |



---

|   |      |
|---|------|
| show debugging snmp .....                           | 1065 |
| show debugging trigger .....                        | 1161 |
| show debugging .....                                | 201  |
| show dhcp lease .....                               | 955  |
| show entity .....                                   | 1264 |
| show exception log .....                            | 315  |
| show file systems .....                             | 98   |
| show file .....                                     | 97   |
| show firewall connections limits config-check ..... | 1231 |
| show firewall connections limits .....              | 1230 |
| show firewall connections .....                     | 1229 |
| show firewall rule config-check .....               | 1234 |
| show firewall rule .....                            | 1232 |
| show firewall .....                                 | 1228 |
| show flowcontrol interface .....                    | 382  |
| show history .....                                  | 60   |
| show hosts .....                                    | 554  |
| show http .....                                     | 163  |
| show interface (PPP) .....                          | 467  |
| show interface brief .....                          | 344  |
| show interface err-disabled .....                   | 383  |
| show interface memory .....                         | 202  |
| show interface memory .....                         | 345  |
| show interface status .....                         | 347  |
| show interface switchport .....                     | 384  |
| show interface tunnel (IPsec) .....                 | 1332 |
| show interface tunnel (IPv6) .....                  | 1393 |
| show interface .....                                | 340  |
| show ip dhcp binding .....                          | 956  |
| show ip dhcp pool .....                             | 958  |
| show ip dhcp server statistics .....                | 964  |
| show ip dhcp server summary .....                   | 966  |
| show ip dhcp-relay .....                            | 1025 |
| show ip dhcp-relay .....                            | 963  |
| show ip dns forwarding cache .....                  | 556  |

---

|                                     |      |
|-------------------------------------|------|
| show ip dns forwarding server ..... | 557  |
| show ip dns forwarding .....        | 555  |
| show ip domain-list .....           | 558  |
| show ip domain-name .....           | 559  |
| show ip flooding-nexthops .....     | 508  |
| show ip interface .....             | 509  |
| show ip name-server .....           | 560  |
| show ip route database .....        | 620  |
| show ip route summary .....         | 621  |
| show ip route .....                 | 618  |
| show ip sockets .....               | 510  |
| show ip traffic .....               | 513  |
| show ips categories .....           | 1294 |
| show ips .....                      | 1293 |
| show ipsec counters .....           | 1333 |
| show ipsec peer .....               | 1334 |
| show ipsec policy .....             | 1335 |
| show ipsec profile .....            | 1336 |
| show ipsec sa .....                 | 1338 |
| show ipv6 dhcp binding .....        | 1027 |
| show ipv6 dhcp interface .....      | 1030 |
| show ipv6 dhcp pool .....           | 1032 |
| show ipv6 dhcp .....                | 1026 |
| show ipv6 forwarding .....          | 605  |
| show ipv6 interface brief .....     | 606  |
| show ipv6 neighbors .....           | 607  |
| show ipv6 route summary .....       | 609  |
| show ipv6 route summary .....       | 623  |
| show ipv6 route .....               | 608  |
| show ipv6 route .....               | 622  |
| show isakmp counters .....          | 1339 |
| show isakmp key (IPsec) .....       | 1340 |
| show isakmp peer .....              | 1341 |
| show isakmp profile .....           | 1342 |
| show isakmp sa .....                | 1344 |

---

|   |      |
|---|------|
| show log config .....                           | 318  |
| show log external.....                          | 320  |
| show log permanent.....                         | 321  |
| show log .....                                  | 316  |
| show mac address-table .....                    | 385  |
| show mac-filter.....                            | 427  |
| show mail .....                                 | 1109 |
| show memory allocations.....                    | 206  |
| show memory history.....                        | 208  |
| show memory pools .....                         | 209  |
| show memory shared.....                         | 210  |
| show memory .....                               | 204  |
| show nat rule config-check .....                | 1286 |
| show nat rule.....                              | 1284 |
| show nat .....                                  | 1283 |
| show ntp associations .....                     | 1052 |
| show ntp counters associations .....            | 1055 |
| show ntp counters.....                          | 1054 |
| show ntp status .....                           | 1056 |
| show ping-poll .....                            | 1205 |
| show platform port.....                         | 389  |
| show platform.....                              | 387  |
| show privilege.....                             | 147  |
| show process.....                               | 211  |
| show reboot history .....                       | 213  |
| show resource.....                              | 166  |
| show router-id.....                             | 214  |
| show running-config atmf .....                  | 882  |
| show running-config firewall.....               | 1236 |
| show running-config interface .....             | 103  |
| show running-config ips .....                   | 1296 |
| show running-config log.....                    | 322  |
| show running-config nat.....                    | 1287 |
| show running-config snmp .....                  | 1066 |
| show running-config software-configuration..... | 1371 |

---

|  |      |
|--|------|
| show running-config ssh.....               | 1130 |
| show running-config trigger .....          | 1162 |
| show running-config url-filter .....       | 1302 |
| show running-config .....                  | 100  |
| show security-password configuration ..... | 148  |
| show security-password user.....           | 149  |
| show snmp-server community .....           | 1068 |
| show snmp-server group .....               | 1069 |
| show snmp-server user .....                | 1070 |
| show snmp-server view.....                 | 1071 |
| show snmp-server .....                     | 1067 |
| show software-configuration .....          | 1372 |
| show ssh server allow-users.....           | 1136 |
| show ssh server deny-users .....           | 1137 |
| show ssh server.....                       | 1134 |
| show ssh .....                             | 1132 |
| show startup-config .....                  | 106  |
| show storm-control.....                    | 391  |
| show system interrupts .....               | 216  |
| show system mac.....                       | 217  |
| show system pci device.....                | 218  |
| show system pci tree .....                 | 219  |
| show system serialnumber.....              | 220  |
| show system usb .....                      | 359  |
| show system .....                          | 215  |
| show tech-support .....                    | 221  |
| show telnet.....                           | 150  |
| show trigger.....                          | 1163 |
| show url-filter .....                      | 1303 |
| show users .....                           | 151  |
| show version .....                         | 107  |
| shutdown .....                             | 349  |
| snmp trap link-status suppress.....        | 1073 |
| snmp trap link-status .....                | 1072 |
| snmp-server community.....                 | 1077 |

---

|                                      |      |
|--------------------------------------|------|
| snmp-server contact                  | 1078 |
| snmp-server enable trap              | 1079 |
| snmp-server engineID local reset     | 1083 |
| snmp-server engineID local           | 1081 |
| snmp-server group                    | 1084 |
| snmp-server host                     | 1086 |
| snmp-server legacy-ifadminstatus     | 1088 |
| snmp-server location                 | 1089 |
| snmp-server source-interface         | 1090 |
| snmp-server startup-trap-delay       | 1091 |
| snmp-server user                     | 1092 |
| snmp-server view                     | 1095 |
| snmp-server                          | 1075 |
| sntp-address                         | 1034 |
| softwire-configuration               | 1374 |
| source-ip                            | 1209 |
| speed (asyn)                         | 223  |
| speed                                | 392  |
| sport                                | 1267 |
| ssh server allow-users               | 1140 |
| ssh server authentication            | 1142 |
| ssh server deny-users                | 1144 |
| ssh server max-auth-tries            | 1146 |
| ssh server resolve-host              | 1147 |
| ssh server scp                       | 1148 |
| ssh server sftp                      | 1149 |
| ssh server                           | 1138 |
| state                                | 883  |
| storm-control level                  | 394  |
| subject-name (ca-trustpoint)         | 645  |
| subnet-mask                          | 967  |
| suppress-ipv4-updates (DDNS)         | 561  |
| switchport atmf-agentlink            | 885  |
| switchport atmf-arealink remote-area | 886  |
| switchport atmf-crosslink            | 888  |

---

|                                       |      |
|---------------------------------------|------|
| switchport atmf-guestlink.....        | 890  |
| switchport atmf-link .....            | 892  |
| tcpdump .....                         | 515  |
| telnet server.....                    | 152  |
| terminal length.....                  | 153  |
| terminal monitor .....                | 225  |
| terminal resize.....                  | 154  |
| test .....                            | 1168 |
| time (trigger) .....                  | 1169 |
| timeout (ping polling) .....          | 1211 |
| traceroute ipv6 .....                 | 610  |
| traceroute.....                       | 516  |
| transform (IPsec Profile).....        | 1345 |
| transform (ISAKMP Profile) .....      | 1346 |
| trap .....                            | 1171 |
| trigger activate .....                | 1173 |
| trigger .....                         | 1172 |
| tunnel destination (DS-Lite).....     | 1376 |
| tunnel destination (IPsec) .....      | 1348 |
| tunnel destination (IPv6).....        | 1394 |
| tunnel dscp .....                     | 1396 |
| tunnel local name (IPsec) .....       | 1350 |
| tunnel local selector .....           | 1351 |
| tunnel mode (IPv6) .....              | 1397 |
| tunnel mode ds-lite.....              | 1377 |
| tunnel mode ipsec.....                | 1353 |
| tunnel mode lw4o6.....                | 1378 |
| tunnel mode map-e .....               | 1379 |
| tunnel protection ipsec (IPsec) ..... | 1354 |
| tunnel remote name (IPsec).....       | 1355 |
| tunnel remote selector.....           | 1356 |
| tunnel security-reprocessing .....    | 1358 |
| tunnel security-reprocessing .....    | 1375 |
| tunnel selector paired .....          | 1359 |
| tunnel software .....                 | 1380 |

---

|                                 |      |
|---------------------------------|------|
| tunnel source (IPsec).....      | 1360 |
| tunnel source (IPv6).....       | 1398 |
| tunnel ttl.....                 | 1400 |
| type atmf node.....             | 1174 |
| type atmf node.....             | 893  |
| type cpu.....                   | 1177 |
| type interface.....             | 1178 |
| type linkmon-probe.....         | 1179 |
| type log.....                   | 1181 |
| type memory.....                | 1182 |
| type periodic.....              | 1183 |
| type ping-poll.....             | 1184 |
| type reboot.....                | 1185 |
| type time.....                  | 1186 |
| type usb.....                   | 1187 |
| undebg (DDNS).....              | 562  |
| undebg all.....                 | 226  |
| undebg atmf.....                | 896  |
| undebg ip packet interface..... | 517  |
| undebg isakmp.....              | 1362 |
| undebg mail.....                | 1110 |
| undebg ping-poll.....           | 1213 |
| undebg platform packet.....     | 395  |
| undebg ppp.....                 | 471  |
| undebg snmp.....                | 1096 |
| undebg ssh server.....          | 1150 |
| undebg trigger.....             | 1188 |
| unmount.....                    | 108  |
| unmount.....                    | 323  |
| up-count.....                   | 1212 |
| update now.....                 | 167  |
| update webgui now.....          | 164  |
| update webgui now.....          | 168  |
| update-interval (DDNS).....     | 563  |
| update-url (DDNS).....          | 564  |

---

|                                       |      |
|---------------------------------------|------|
| upstream-interface .....              | 1381 |
| url-filter reload custom-lists .....  | 1304 |
| url-filter .....                      | 1305 |
| usb mode-switch .....                 | 361  |
| use-ipv4-for-ipv6-updates (DDNS)..... | 567  |
| username (DDNS).....                  | 568  |
| username .....                        | 155  |
| username .....                        | 897  |
| version (ISAKMP) .....                | 1363 |
| wait .....                            | 327  |
| whitelist (url-filter).....           | 1306 |
| write file.....                       | 109  |
| write memory .....                    | 110  |
| write terminal .....                  | 111  |
| zone .....                            | 1269 |



# Part 1: Setup and Troubleshooting

# 1

# CLI Navigation Commands

## Introduction

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

- Command List**
- “[configure terminal](#)” on page 51
  - “[disable \(Privileged Exec mode\)](#)” on page 52
  - “[do](#)” on page 53
  - “[enable \(Privileged Exec mode\)](#)” on page 54
  - “[end](#)” on page 56
  - “[exit](#)” on page 57
  - “[help](#)” on page 58
  - “[logout](#)” on page 59
  - “[show history](#)” on page 60

# configure terminal

**Overview** This command enters the Global Configuration command mode.

**Syntax** `configure terminal`

**Mode** Privileged Exec

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

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

# disable (Privileged Exec mode)

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

**Syntax** `disable`

**Mode** Privileged Exec

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

```
awplus# disable
awplus>
```

**Related commands**

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

# do

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

**Syntax** `do <command>`

| Parameter                    | Description                             |
|------------------------------|---|
| <code>&lt;command&gt;</code> | Specify the command and its parameters. |

**Mode** Any configuration mode

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

# enable (Privileged Exec mode)

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

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

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

**Mode** User Exec

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

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

Note that a separate password can be configured for each privilege level using the [enable password](#) and the [enable secret](#) 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 eth1
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 the **exit** command to exit Interface mode, and return to Configure mode.

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# exit
awplus(config)#
```

**Related commands**

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

# help

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

**Syntax** help

**Mode** All command modes

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

```
awplus# help
```

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

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

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

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

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

# logout

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

**Syntax** `logout`

**Mode** User Exec and Privileged Exec

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

```
awplus# logout
```

# show history

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

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

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

**Syntax** `show history`

**Mode** User Exec and Privileged Exec

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

```
awplus# show history
```

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

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

# 2

# File and Configuration Management Commands

## Introduction

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

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

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

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

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

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

**Syntax for directory listings**

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

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

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

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

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

**Command List**

- ["autoboot enable"](#) on page 64
- ["boot config-file"](#) on page 65
- ["boot config-file backup"](#) on page 67
- ["boot system"](#) on page 68

- [“boot system backup”](#) on page 69
- [“cd”](#) on page 70
- [“copy \(filename\)”](#) on page 71
- [“copy current-software”](#) on page 73
- [“copy debug”](#) on page 74
- [“copy running-config”](#) on page 75
- [“copy startup-config”](#) on page 76
- [“copy zmodem”](#) on page 77
- [“create autoboot”](#) on page 78
- [“delete”](#) on page 79
- [“delete debug”](#) on page 80
- [“dir”](#) on page 81
- [“edit”](#) on page 83
- [“edit \(filename\)”](#) on page 84
- [“erase factory-default”](#) on page 85
- [“erase startup-config”](#) on page 86
- [“ip tftp source-interface”](#) on page 87
- [“ipv6 tftp source-interface”](#) on page 88
- [“mkdir”](#) on page 89
- [“move”](#) on page 90
- [“move debug”](#) on page 91
- [“pwd”](#) on page 92
- [“rmdir”](#) on page 93
- [“show autoboot”](#) on page 94
- [“show boot”](#) on page 95
- [“show file”](#) on page 97
- [“show file systems”](#) on page 98
- [“show running-config”](#) on page 100
- [“show running-config interface”](#) on page 103
- [“show startup-config”](#) on page 106
- [“show version”](#) on page 107
- [“unmount”](#) on page 108
- [“write file”](#) on page 109
- [“write memory”](#) on page 110
- [“write terminal”](#) on page 111

# autoboot enable

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

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

Figure 2-1: Example `autoboot.txt` file

```
[AlliedWare Plus]
Copy_from_external_media_enabled=yes
Boot_Release=AR1050V-5.5.0-0.1.rel
Boot_Config=network1.cfg
```

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

**Syntax** `autoboot enable`  
`no autoboot enable`

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

**Mode** Global Configuration

**Example** To enable the Autoboot feature, use the command:

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

**Related commands** [create autoboot](#)  
[show autoboot](#)  
[show boot](#)



# boot config-file

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

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

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

**Mode** Global Configuration

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

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

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

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

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

To stop running the configuration file "branch.cfg" when the device boots up, when "branch.cfg" is stored on the device's Flash filesystem, use the commands:

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

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

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

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

```
awplus# configure terminal
```

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

**Related  
commands**

[boot config-file backup](#)

[boot system](#)

[boot system backup](#)

[show boot](#)

# boot config-file backup

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

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

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

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

**Mode** Global Configuration

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

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

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

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

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

**Related commands**

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

# boot system

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

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

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

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

**Mode** Global Configuration

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

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

**Examples** To boot up with the release file AR1050V-5.5.0-0.1.rel the next time the device boots up, when the release file is stored on the device's flash filesystem, use the commands:

```
awplus# configure terminal  
awplus(config)# boot system flash:/AR1050V-5.5.0-0.1.rel
```

To run the release file AR1050V-5.5.0-0.1.rel the next time the device boots up, when the release file is stored on a USB storage device, use the commands:

```
awplus# configure terminal  
awplus(config)# boot system usb:/AR1050V-5.5.0-0.1.rel
```

**Related commands**

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

# boot system backup

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

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

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

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

**Mode** Global Configuration

**Examples** To specify the file AR1050V-5.4.9-2.1.rel as the backup to the main release file, use the commands:

```
awplus# configure terminal  
awplus(config)# boot system backup flash:/AR1050V-5.4.9-2.1.rel
```

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

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

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

# cd

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

**Syntax** `cd <directory-name>`

| Parameter                           | Description                     |
|-------------------------------------|---------------------------------|
| <code>&lt;directory-name&gt;</code> | Name and path of the directory. |

**Mode** Privileged Exec

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

```
awplus# cd images
```

**Related commands**

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

# copy (filename)

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

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

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

| Parameter                             | Description  |
|---------------------------------------|--|
| <code>force</code>                    | This parameter forces the copy command to overwrite the destination file, if it already exists, without prompting the user for confirmation. |
| <code>&lt;source-name&gt;</code>      | The filename and path of the source file. See <a href="#">Introduction</a> on page 61 for valid syntax.                                      |
| <code>&lt;destination-name&gt;</code> | The filename and path for the destination file. See <a href="#">Introduction</a> on page 61 for valid syntax.                                |

**Mode** Privileged Exec

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

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

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

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

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

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

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

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

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

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

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

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

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

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

On an AMF network, to copy the device GUI file from the AMF master to the Flash memory of 'node\_1', use the command:

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

**Related  
commands**

[copy zmodem](#)

[copy buffered-log](#)

[copy permanent-log](#)

[edit \(filename\)](#)

[show file systems](#)



# copy current-software

**Overview** This command copies the AlliedWare Plus™ OS software that the device has booted from, to a destination file.

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

| Parameter                             | Description  |
|---------------------------------------|--|
| <code>&lt;destination-name&gt;</code> | The filename and path where you would like the current running-release saved. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See <a href="#">Introduction</a> on page 61 for valid syntax. |

**Mode** Privileged Exec

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

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

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

# copy debug

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

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

| Parameter                             | Description  |
|---------------------------------------|--|
| <code>&lt;destination-name&gt;</code> | The filename and path where you would like the debug output saved. See <a href="#">Introduction</a> on page 61 for valid syntax. |
| <code>&lt;source-name&gt;</code>      | The filename and path where the debug output originates. See the <a href="#">Introduction</a> to this chapter for valid syntax.  |

**Mode** Privileged Exec

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

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

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

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

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

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

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

# copy running-config

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

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

| Parameter                             | Description  |
|---------------------------------------|--|
| <code>&lt;source-name&gt;</code>      | The filename and path of a configuration file. This must be a valid configuration file with a <b>.cfg</b> filename extension. Specify this when you want the script in the file to become the new running-config. See <a href="#">Introduction</a> on page 61 for valid syntax.  |
| <code>&lt;destination-name&gt;</code> | The filename and path where you would like the current running-config saved. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See <a href="#">Introduction</a> on page 61 for valid syntax. If you do not specify a file name, the device saves the running-config to a file called default.cfg. |
| <code>startup-config</code>           | Copies the running-config into the file set as the current startup-config file.  |

**Mode** Privileged Exec

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

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

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

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

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

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

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

# copy startup-config

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

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

| Parameter                             | Description  |
|---------------------------------------|--|
| <code>&lt;source-name&gt;</code>      | The filename and path of a configuration file. This must be a valid configuration file with a <b>.cfg</b> 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 <a href="#">Introduction</a> on page 61 for valid syntax. |
| <code>&lt;destination-name&gt;</code> | The destination and filename that you are saving the startup-config as. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See <a href="#">Introduction</a> on page 61 for valid syntax.   |

**Mode** Privileged Exec

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

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

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

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

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

# copy zmodem

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

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

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;source-name&gt;</code> | The filename and path of the source file. See <a href="#">Introduction</a> on page 61 for valid syntax. |

**Mode** Privileged Exec

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

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

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

# create autoboot

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

**Syntax** `create autoboot usb`

**Mode** Privileged Exec

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

```
awplus# create autoboot usb
```

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

# delete

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

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

| Parameter                     | Description  |
|-------------------------------|--|
| <code>force</code>            | Ignore nonexistent filenames and never prompt before deletion.   |
| <code>recursive</code>        | Remove the contents of directories recursively.  |
| <code>&lt;filename&gt;</code> | The filename and path of the file to delete. See <a href="#">Introduction</a> on page 61 for valid syntax. |

**Mode** Privileged Exec

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

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

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

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

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

```
awplus# delete recursive old_configs
```

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

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

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

# delete debug

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

**Syntax** delete debug <source-name>

| Parameter     | Description  |
|---------------|--|
| <source-name> | The filename and path where the debug output originates. See <a href="#">Introduction</a> on page 61 for valid URL syntax. |

**Mode** Privileged Exec

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

```
awplus# delete debug
```

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

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

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



# dir

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

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

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

**Mode** Privileged Exec

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

```
awplus# dir
```

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

```
awplus# dir flash
```

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

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

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

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

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

```
awplus# dir sort name
```

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

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

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

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

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

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

**Related commands** [cd](#)  
[pwd](#)

# edit

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

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

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

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

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

**Syntax** `edit [<filename>]`

| Parameter                     | Description                                   |
|-------------------------------|---|
| <code>&lt;filename&gt;</code> | Name of a file in the local Flash filesystem. |

**Mode** Privileged Exec

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

```
awplus# edit
```

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

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

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

# edit (filename)

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

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

**Syntax** `edit <filename>`

| Parameter                     | Description   |
|-------------------------------|---|
| <code>&lt;filename&gt;</code> | The filename and path of the remote file. See <a href="#">Introduction</a> on page 61 for valid syntax. |

**Mode** Privileged Exec

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

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

**Related commands**

- [copy \(filename\)](#)
- [edit](#)
- [show file](#)

# erase factory-default

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

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

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

**Syntax** `erase factory-default`

**Mode** Privileged Exec.

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

**Example** To erase data, use the command:

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

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

**Related commands** [atmf cleanup](#)

# erase startup-config

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

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

**Syntax** `erase startup-config`

**Mode** Privileged Exec

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

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

**Related commands**

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

# ip tftp source-interface

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

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

**Syntax** `ip tftp source-interface [<interface>|<ip-add>]`  
`no ip tftp source-interface`

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

**Default** There is no default source specified.

**Mode** Global Configuration

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

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

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

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

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

# ipv6 tftp source-interface

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

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

**Syntax** `ipv6 tftp source-interface [<interface>|<ipv6-add>]`  
`no ipv6 tftp source-interface`

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

**Default** There is no default source specified.

**Mode** Global Configuration

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

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

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

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

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



# mkdir

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

**Syntax** `mkdir <name>`

| Parameter                 | Description   |
|---------------------------|---|
| <code>&lt;name&gt;</code> | The name and path of the directory that you are creating. |

**Mode** Privileged Exec

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

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

```
awplus# mkdir images
```

**Related commands** `cd`  
`dir`  
`pwd`

# move

**Overview** This command renames or moves a file.

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

| Parameter                             | Description  |
|---------------------------------------|--|
| <code>&lt;source-name&gt;</code>      | The filename and path of the source file. See <a href="#">Introduction</a> on page 61 for valid syntax.      |
| <code>&lt;destination-name&gt;</code> | The filename and path of the destination file. See <a href="#">Introduction</a> on page 61 for valid syntax. |

**Mode** Privileged Exec

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

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

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

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

**Related commands** [delete](#)  
[edit](#)

[show file](#)

[show file systems](#)

# move debug

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

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

| Parameter                             | Description   |
|---------------------------------------|---|
| <code>&lt;destination-name&gt;</code> | The filename and path where you would like the debug output moved to. See <a href="#">Introduction</a> on page 61 for valid syntax. |

**Mode** Privileged Exec

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

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

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 2-5: CLI prompt after entering the **move debug** command

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

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

# pwd

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

**Syntax** `pwd`

**Mode** Privileged Exec

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

```
awplus# pwd
```

**Related commands** `cd`

# rmdir

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

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

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

**Mode** Privileged Exec

**Usage notes** You can use the CLI to access filesystems on a specific external memory device. See the [Introduction](#) on page 61 for syntax details.

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

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

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

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

**Related commands**

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

# show autoboot

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

**Syntax** show autoboot

**Mode** Privileged Exec

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

```
awplus# show autoboot
```

**Output** Figure 2-6: Example output from the **show autoboot** command

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

Restore information on USB
Autoboot enable in autoboot.txt : yes
Restore release file       : AR1050V-5.5.0-0.1.rel (file exists)
Restore configuration file  : network_1.cfg (file exists)
```

Figure 2-7: Example output from the **show autoboot** command when an external media source is not present

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

**Related commands**

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

# show boot

**Overview** This command displays the current boot configuration. We recommend that the currently running release is set as the current boot image.

**Syntax** show boot

**Mode** Privileged Exec

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

```
awplus# show boot
```

**Output** Figure 2-8: Example output from **show boot** when the current boot config is on a USB storage device

```
awplus#show boot
Boot configuration
-----
Current software   : AR1050V-5.5.0-0.1.rel
Current boot image : usb:/AR1050V-5.5.0-0.1.rel
Backup boot image  : flash:/AR1050V-5.4.9-2.1.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
```

Table 2-1: Parameters in the output from **show boot**

| Parameter           | Description  |
|---------------------|--|
| Current software    | The current software release that the device is using.   |
| Current boot image  | The boot image currently configured for use during the next boot cycle.  |
| Backup boot image   | The boot image to use during the next boot cycle if the device cannot load the main image.   |
| Default boot config | The default startup configuration file. The device loads this configuration script if no file is set as the startup-config file.                                 |
| Current boot config | The configuration file currently configured as the startup-config file. The device loads this configuration file during the next boot cycle if this file exists. |

Table 2-1: Parameters in the output from **show boot** (cont.)

| Parameter          | Description   |
|--------------------|---|
| Backup boot config | The configuration file to use during the next boot cycle if the main configuration file cannot be loaded. |
| Autoboot status    | The status of the Autoboot feature; either enabled or disabled.   |

**Related commands**

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



# show file

**Overview** This command displays the contents of a specified file.

**Syntax** `show file <filename>`

| Parameter                     | Description   |
|-------------------------------|---|
| <code>&lt;filename&gt;</code> | Name of a file on the local Flash filesystem, or name and directory path of a file. |

**Mode** Privileged Exec

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

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

**Related commands**

- [edit](#)
- [edit \(filename\)](#)
- [show file systems](#)

# show file systems

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

**Syntax** `show file systems`

**Mode** Privileged Exec

**Examples** To display the filesystems, use the command:

```
awplus# show file systems
```

**Output** Figure 2-9: Example output from the **show file systems** command

```
AR1050V#show file systems
```

| Size(b) | Free(b) | Type     | Flags | Prefixes | S/D/V   | Lcl/Ntwk | Avail |
|---------|---------|----------|-------|----------|---------|----------|-------|
| 106.4M  | 35.6M   | flash    | rw    | flash:   | static  | local    | Y     |
| -       | -       | system   | rw    | system:  | virtual | local    | -     |
| 10.0M   | 9.9M    | debug    | rw    | debug:   | static  | local    | Y     |
| -       | -       | usbstick | rw    | usb:     | dynamic | local    | N     |
| -       | -       | fserver  | rw    | fserver: | dynamic | network  | N     |
| -       | -       | tftp     | rw    | tftp:    | -       | network  | -     |
| -       | -       | scp      | rw    | scp:     | -       | network  | -     |
| -       | -       | sftp     | ro    | sftp:    | -       | network  | -     |
| -       | -       | http     | ro    | http:    | -       | network  | -     |
| -       | -       | rsync    | rw    | rsync:   | -       | network  | -     |

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

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

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

| Parameter  | Description  |
|------------|--|
| Prefixes   | The prefixes used when entering commands to access the filesystems, such as:<br>flash<br>system<br>usb<br>tftp<br>scp<br>sftp<br>http. |
| S/V/D      | The memory type: static, virtual, dynamic.   |
| Lcl / Ntwk | Whether the memory is located locally or via a network connection.   |
| Avail      | Whether the memory is accessible: Y (yes), N (no), - (not applicable)  |

**Related commands**

- [edit](#)
- [edit \(filename\)](#)
- [show file](#)

# show running-config

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

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

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

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

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

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

| Parameter   | Description               |
|-------------|---------------------------|
| switch      | Switch configuration      |
| web-control | Web Control configuration |

**Mode** Privileged Exec and Global Configuration

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

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

**Output** Figure 2-10: Example output from **show running-config**

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

...

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

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

# show running-config interface

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

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

**Syntax** `show running-config interface [<interface-list>]`

| Parameter                           | Description   |
|-------------------------------------|---|
| <code>&lt;interface-list&gt;</code> | The interfaces or ports to display information about. An interface-list can be: <ul style="list-style-type: none"><li>• a PPP interface (e.g. ppp0)</li><li>• an Eth interface (e.g. eth1)</li><li>• vlan1</li><li>• a switchport (e.g. port1.0.4)</li><li>• a bridge interface (e.g. br0)</li><li>• a tunnel interface (e.g. tunnel0)</li><li>• a 3G cellular interface (e.g. cellular0)</li><li>• a WWAN interface (e.g. wwan0)</li><li>• the loopback interface (lo)</li><li>• a continuous range of interfaces, separated by a hyphen (e.g. ppp2-4)</li><li>• a comma-separated list (e.g. ppp0,ppp2-4). Do not mix interface types in a list.</li></ul> The specified interfaces must exist. |
| <code>dot1x</code>                  | Displays running configuration for 802.1X port authentication for the specified interfaces.   |
| <code>lacp</code>                   | Displays running configuration for LACP (Link Aggregation Control Protocol) for the specified interfaces.   |
| <code>ip igmp</code>                | Displays running configuration for IGMP (Internet Group Management Protocol) for the specified interfaces.  |
| <code>ip multicast</code>           | Displays running configuration for general multicast settings for the specified interfaces.   |
| <code>ip pim sparse-mode</code>     | Displays running configuration for PIM-SM (Protocol Independent Multicast - Sparse Mode) for the specified interfaces.  |
| <code>ip pim dense-mode</code>      | Displays running configuration for PIM-DM (Protocol Independent Multicasting - Dense Mode) for the specified interfaces.  |
| <code>mstp</code>                   | Displays running configuration for MSTP (Multiple Spanning Tree Protocol) for the specified interfaces.   |

| Parameter | Description  |
|-----------|--|
| ospf      | Displays running configuration for OSPF (Open Shortest Path First) for the specified interfaces.     |
| rip       | Displays running configuration for RIP (Routing Information Protocol) for the specified interfaces.  |
| ipv6 rip  | Displays running configuration for RIPng (RIP for IPv6) for the specified interfaces.                |
| rstp      | Displays running configuration for RSTP (Rapid Spanning Tree Protocol) for the specified interfaces. |
| stp       | Displays running configuration for STP (Spanning Tree Protocol) for the specified interfaces.        |

**Mode** Privileged Exec and Global Configuration

**Default** Displays information for all protocols on all interfaces

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

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

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

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

To display the current running configuration of a device for vlan1, use the command:

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

**Output** Figure 2-11: Example output from a **show running-config interface ppp0** command

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

Figure 2-12: Example output from **show running-config interface** for a switchport

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



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

# show startup-config

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

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

**Syntax** show startup-config

**Mode** Privileged Exec

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

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

**Output** Figure 2-13: Example output from the **show startup-config** command

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

...

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

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

# show version

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

**Syntax** `show version`

**Mode** User Exec and Privileged Exec

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

```
awplus# show version
```

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

# unmount

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

**Syntax** `unmount usb`

| Parameter | Description                     |
|-----------|---------------------------------|
| usb       | Unmount the USB storage device. |

**Mode** Privileged Exec

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

```
awplus# unmount usb
```

**Related commands**

- [clear log external](#)
- [log external](#)
- [show file systems](#)
- [show log config](#)
- [show log external](#)

**Command changes** Version 5.4.7-1.1: command added

# write file

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

**Syntax** write [file]

**Mode** Privileged Exec

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

```
awplus# write file
```

**Related commands**

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

# write memory

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

**Syntax** write [memory]

**Mode** Privileged Exec

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

```
awplus# write memory
```

**Related commands**

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

# write terminal

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

**Syntax** write terminal

**Mode** Privileged Exec

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

```
awplus# write terminal
```

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

# 3

# User Access Commands

## Introduction

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

- Command List**
- “aaa authentication enable default local” on page 114
  - “aaa local authentication attempts lockout-time” on page 115
  - “aaa local authentication attempts max-fail” on page 116
  - “aaa login fail-delay” on page 117
  - “clear aaa local user lockout” on page 118
  - “clear line console” on page 119
  - “clear line vty” on page 120
  - “enable password” on page 121
  - “enable secret” on page 124
  - “exec-timeout” on page 127
  - “flowcontrol hardware (asyn/console)” on page 129
  - “length (asyn)” on page 131
  - “line” on page 132
  - “privilege level” on page 134
  - “security-password history” on page 135
  - “security-password forced-change” on page 136
  - “security-password lifetime” on page 137
  - “security-password min-lifetime-enforce” on page 138
  - “security-password minimum-categories” on page 139
  - “security-password minimum-length” on page 140



- [“security-password reject-expired-pwd”](#) on page 141
- [“security-password warning”](#) on page 142
- [“service advanced-vty”](#) on page 143
- [“service password-encryption”](#) on page 144
- [“service telnet”](#) on page 145
- [“show aaa local user locked”](#) on page 146
- [“show privilege”](#) on page 147
- [“show security-password configuration”](#) on page 148
- [“show security-password user”](#) on page 149
- [“show telnet”](#) on page 150
- [“show users”](#) on page 151
- [“telnet server”](#) on page 152
- [“terminal length”](#) on page 153
- [“terminal resize”](#) on page 154
- [“username”](#) on page 155

# aaa authentication enable default local

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

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

**Default** Local privilege level authentication is enabled by default.

**Mode** Global Configuration

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

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

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

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

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

**Related commands** [enable \(Privileged Exec mode\)](#)  
[enable password](#)  
[enable secret](#)

# aaa local authentication attempts lockout-time

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

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

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

| Parameter                         | Description   |
|-----------------------------------|---|
| <code>&lt;lockout-time&gt;</code> | <code>&lt;0-10000&gt;</code> . Time in seconds to lockout the user. |

**Mode** Global Configuration

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

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

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

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

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

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

**Related commands** [aaa local authentication attempts max-fail](#)

# aaa local authentication attempts max-fail

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

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

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

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

**Mode** Global Configuration

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

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

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

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

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

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

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

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

# aaa login fail-delay

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

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

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

**Default** 1 second

**Mode** Global configuration

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

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

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

# clear aaa local user lockout

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

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

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

**Mode** Privileged Exec

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

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

To unlock all user accounts use the following command:

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

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

# clear line console

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

**Syntax** `clear line console 0`

**Mode** Privileged Exec

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

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

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

**Related commands**

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

# clear line vty

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

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

| Parameter | Description |
|-----------|-------------|
| <0-32>    | Line number |

**Mode** Privileged Exec

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

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

**Related commands**

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



# enable password

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

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

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

| Parameter                   | Description   |
|-----------------------------|---|
| <code>&lt;plain&gt;</code>  | Specifies the unencrypted password.   |
| 8                           | Specifies a hidden password will follow.  |
| <code>&lt;hidden&gt;</code> | Specifies the hidden encrypted password. Use an encrypted password for better security where a password crosses the network or is stored on a TFTP server.  |
| level                       | Privilege level <1-15>. Level for which the password applies. You can specify up to 16 privilege levels, using numbers 1 through 15. Level 1 is normal EXEC-mode user privileges for User Exec mode. If this argument is not specified in the command or the <b>no</b> variant of the command, the privilege level defaults to 15 (enable mode privileges) for Privileged Exec mode. A privilege level of 7 can be set for intermediate CLI security. |

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

**Mode** Global Configuration

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

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

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

### Using plain passwords

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

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

This results in the following show output:

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

### Using encrypted passwords

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

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

This results in the following show output:

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

### Using hidden passwords

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

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

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

This results in the following show output:

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

**Related commands**

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

# enable secret

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

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

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

| Parameter                   | Description   |
|-----------------------------|---|
| <code>&lt;plain&gt;</code>  | Specifies the unencrypted password.   |
| 8                           | Specifies a hidden password will follow.  |
| <code>&lt;hidden&gt;</code> | Specifies the hidden encrypted password. Use an encrypted password for better security where a password crosses the network or is stored on a TFTP server.  |
| level                       | Privilege level <1-15>. Level for which the password applies. You can specify up to 16 privilege levels, using numbers 1 through 15. Level 1 is normal EXEC-mode user privileges for User Exec mode. If this argument is not specified in the command or the <b>no</b> variant of the command, the privilege level defaults to 15 (enable mode privileges) for Privileged Exec mode. A privilege level of 7 can be set for intermediate CLI security. |

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

**Mode** Global Configuration

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

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

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

### Using plain passwords

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

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

This results in the following show output:

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

### Using encrypted passwords

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

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

This results in the following show output:

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

### Using hidden passwords

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

The output in the configuration file will show only the encrypted string, and not the text string:

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

This results in the following show output:

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

**Related commands**

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

# exec-timeout

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

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

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

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

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

**Mode** Line Configuration

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

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

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

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

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

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

**Validation Commands** `show running-config`

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



# flowcontrol hardware (asyn/console)

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

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

**Mode** Line Configuration

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

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

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

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

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

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

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

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

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

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

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

**Related commands**

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

# length (asyn)

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

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

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

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

**Mode** Line Configuration

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

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

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

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

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

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

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

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

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

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

# line

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

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

| Parameter                       | Description  |
|---------------------------------|--|
| <code>&lt;first-line&gt;</code> | <code>&lt;0-32&gt;</code> Specify the first line number. |
| <code>&lt;last-line&gt;</code>  | <code>&lt;0-32&gt;</code> Specify the last line number.  |
| <code>console</code>            | The console terminal line(s) for local access.           |
| <code>vty</code>                | Virtual terminal for remote console access.              |

**Mode** Global Configuration

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

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**

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

# privilege level

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

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

**Mode** Line Configuration

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

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

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

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

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

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

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

**Related commands**

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

# security-password history

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

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

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

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

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

**Mode** Global Configuration

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

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

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

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

**Related commands**

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

# security-password forced-change

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

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

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

**Syntax** security-password forced-change  
no security-password forced-change

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

**Mode** Global Configuration

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

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

**Related commands**

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



# security-password lifetime

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

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

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

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

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

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

**Mode** Global Configuration

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

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

**Related commands**

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

# security-password min-lifetime-enforce

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

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

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

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

**Default** By default, no minimum lifetime is enforced.

**Mode** Global Configuration

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

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

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

**Related commands**

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

**Command changes** Version 5.4.7-0.2: command added

# security-password minimum-categories

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

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

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

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

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

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

**Mode** Global Configuration

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

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

**Related commands**

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

# security-password minimum-length

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

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

| Parameter                 | Description  |
|---------------------------|--|
| <code>&lt;1-23&gt;</code> | Minimum password length in the range from 1 to 23. |

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

**Mode** Global Configuration

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

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

**Related commands**

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

# security-password reject-expired-pwd

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

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

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

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

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

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

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

**Mode** Global Configuration

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

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

**Related commands**

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

# security-password warning

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

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

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

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

| Parameter                   | Description  |
|-----------------------------|--|
| <code>&lt;0-1000&gt;</code> | 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 <b>no security-password warning</b> command. The warning period must be less than, or equal to, the password lifetime set with the <a href="#">security-password lifetime</a> command. |

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

**Mode** Global Configuration

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

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

**Related commands**

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

# service advanced-vty

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

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

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

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

**Mode** Global Configuration

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

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

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

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

# service password-encryption

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

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

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

**Mode** Global Configuration

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

**Validation Commands** `show running-config`

**Related commands** `enable password`



# service telnet

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

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

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

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

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

**Mode** Global Configuration

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

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

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

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

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

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

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

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

**Related commands**

- [clear line vty](#)
- [show telnet](#)
- [telnet server](#)

# show aaa local user locked

**Overview** This command displays the 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 3-1: Example output from the **show aaa local user locked** command

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

**Related commands**

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

# show privilege

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

**Syntax** `show privilege`

**Mode** User Exec and Privileged Exec

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

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

```
awplus# show privilege
```

**Output** Figure 3-2: Example output from the **show privilege** command

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

**Related commands** [privilege level](#)

# show security-password configuration

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

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

**Mode** Privileged Exec

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

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

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

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

- Related commands**
- [security-password forced-change](#)
  - [security-password history](#)
  - [security-password lifetime](#)
  - [security-password min-lifetime-enforce](#)
  - [security-password minimum-categories](#)
  - [security-password minimum-length](#)
  - [security-password reject-expired-pwd](#)
  - [security-password warning](#)
  - [show security-password user](#)

# show security-password user

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

**Syntax** show security-password user

**Mode** Privileged Exec

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

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

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

| User account and password information |           |                 |                    |
|---------------------------------------|-----------|-----------------|--------------------|
| UserName                              | Privilege | Last-PWD-Change | Remaining-lifetime |
| manager                               | 15        | 4625 day(s) ago | No Expiry          |
| bob15                                 | 15        | 0 day(s) ago    | 30 days            |
| ted7                                  | 7         | 0 day(s) ago    | No Expiry          |
| mike1                                 | 1         | 0 day(s) ago    | No Expiry          |

- Related commands**
- [security-password forced-change](#)
  - [security-password history](#)
  - [security-password lifetime](#)
  - [security-password min-lifetime-enforce](#)
  - [security-password minimum-categories](#)
  - [security-password minimum-length](#)
  - [security-password reject-expired-pwd](#)
  - [security-password warning](#)
  - [show security-password configuration](#)

# show telnet

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

**Syntax** show telnet

**Mode** User Exec and Privileged Exec

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

```
awplus# show telnet
```

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

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

**Related commands**

- [clear line vty](#)
- [service telnet](#)
- [show users](#)
- [telnet server](#)

# show users

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

**Syntax** `show users`

**Mode** User Exec and Privileged Exec

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

```
awplus# show users
```

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

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

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

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

# telnet server

**Overview** This command enables the telnet server on the specified TCP port. If the server is already enabled then it will be restarted on the new port. Changing the port number does not affect the port used by existing sessions.

**Syntax** `telnet server {<1-65535>|default}`

| Parameter | Description                         |
|-----------|-------------------------------------|
| <1-65535> | The TCP port to listen on.          |
| default   | Use the default TCP port number 23. |

**Mode** Global Configuration

**Example** To enable the telnet server on TCP port 2323, use the following commands:

```
awplus# configure terminal
awplus(config)# telnet server 2323
```

**Related commands** [show telnet](#)



# terminal length

**Overview** Use the **terminal length** command to specify the number of rows of output that the device will display before pausing, for the currently-active terminal only.

Use the **terminal no length** command to remove the length specified by this command. The default length will apply unless you have changed the length for some or all lines by using the [length \(asyn\)](#) command.

**Syntax** `terminal length <length>`  
`terminal no length [<length>]`

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

**Mode** User Exec and Privileged Exec

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

```
awplus# terminal length 15
```

The following example removes terminal length set previously:

```
awplus# terminal no length
```

**Related commands** [terminal resize](#)  
[length \(asyn\)](#)

# terminal resize

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

**Syntax** `terminal resize`

**Mode** User Exec and Privileged Exec

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

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

```
awplus# terminal resize
```

**Related commands** [length \(asyn\)](#)  
[terminal length](#)

# username

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

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

**Syntax**

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

| Parameter | Description  |
|-----------|--|
| <name>    | The login name for the user. Do not use punctuation marks such as single quotes ('), double quotes ("), or colons (:) with the user login name.  |
| privilege | The user's privilege level. Use the privilege levels to set the access rights for each user.<br><br><1-15> A privilege level: either 1-14 (limited access) or 15 (full access). A user with privilege level 1-14 can only access higher privilege levels if an <a href="#">enable password</a> has been configured for the level the user tries to access and the user enters that password.<br>A user at privilege level 1 can access the majority of show commands. A user at privilege level 7 can access the majority of show commands including platform show commands. Privilege Level 15 (to access the Privileged Exec command mode) is required to access configuration commands as well as show commands in Privileged Exec. |
| password  | A password that the user must enter when logging in.<br><br>8 Specifies that you are entering a password as a string that has already been encrypted, instead of entering a plain-text password. The running-config displays the new password as an encrypted string even if password encryption is turned off. Note that the user enters the plain-text version of the password when logging in.  |
|           | <password> The user's password. The password can be up to 32 characters in length and include characters from up to four categories. The password categories are: <ul style="list-style-type: none"> <li>uppercase letters: A to Z</li> <li>lowercase letters: a to z</li> <li>digits: 0 to 9</li> <li>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.</li> </ul>  |

**Mode** Global Configuration

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

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

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

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

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

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

**Related commands** [enable password](#)  
[security-password minimum-categories](#)  
[security-password minimum-length](#)

# 4

# GUI Commands

## Introduction

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

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

- Command List**
- [“atmf topology-gui enable”](#) on page 158
  - [“http port”](#) on page 159
  - [“http secure-port”](#) on page 160
  - [“log event-host”](#) on page 161
  - [“service http”](#) on page 162
  - [“show http”](#) on page 163
  - [“update webgui now”](#) on page 164

# atmf topology-gui enable

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

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

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

**Syntax** atmf topology-gui enable  
no atmf topology-gui enable

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

**Mode** Global Configuration mode

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

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

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

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

**Example** To enable Vista Manager EX on Node1, use the following commands:

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

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

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

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

# http port

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

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

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

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

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

**Mode** Global Configuration

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

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

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

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

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

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

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

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

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

# http secure-port

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

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

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

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

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

**Mode** Global Configuration

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

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

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

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

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

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

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

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

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

**Command changes** Version 5.4.7-1.1: command added on AR-Series devices  
Version 5.4.7-2.4: **none** parameter added

Version 5.4.8-0.2: command added on AlliedWare Plus switches



# log event-host

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

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

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

| Parameter                      | Description                    |
|--------------------------------|--------------------------------|
| <code>&lt;ipv4-addr&gt;</code> | ipv4 address of the event host |
| <code>&lt;ipv6-addr&gt;</code> | ipv6 address of the event host |

**Default** Log events are disabled by default.

**Mode** Global Configuration

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

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

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

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

```
Node1# configure terminal
```

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

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

```
Node1# configure terminal
```

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

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

# service http

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

**Syntax** `service http`  
`no service http`

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

**Mode** Global Configuration

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

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

To disable the HTTP service, use the following commands:

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

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

# show http

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

**Syntax** show http

**Mode** User Exec and Privileged Exec

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

```
awplus# show http
```

**Output** Figure 4-1: Example output from the **show http** command

```
awplus#show http
HTTP Server Configuration
-----
HTTP server           : Enabled
Port                  : 80
Web GUI Information
-----
GUI file in use       : webgui
GUI version:          : 3.1
```

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

# update webgui now

**Overview** Use this command to check whether you have the latest version of the device's GUI and update it if a newer version is available.

**Syntax** `update webgui now`

**Mode** Privileged Exec

**Usage notes** This command applies since software version 5.4.6-1.1. Prior to 5.4.6-1.1, users used the **copy** command to copy GUI files onto the AR-series firewall instead. If you did that, you need to delete all GUI files from Flash memory before you run the "update webgui now" command. To delete all GUI files, use the command:

```
awplus#del *gui_*.tar.gz
```

**Examples** To check for GUI updates, use the following command:

```
awplus#update webgui now
```

**Related commands** [show resource](#)

# 5

# Update Manager Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to update a resource. For more information, see the [Update Manager Feature Overview and Configuration\\_Guide](#).

- Command List**
- “[show resource](#)” on page 166
  - “[update now](#)” on page 167
  - “[update webgui now](#)” on page 168

# show resource

**Overview** Use this command to show information about the resources of features that have been enabled.

**Syntax** `show resource [<resource_name>]`

| Parameter                          | Description               |
|------------------------------------|---------------------------|
| <code>&lt;resource_name&gt;</code> | Specific resource to show |

**Mode** Privileged Exec

**Examples** To show information about the resources of features that have been enabled, use the following command:

```
awplus#show resource
```

**Output** Figure 5-1: Example **show resource** output

```
awplus#show resource
```

| Resource Name  | Status   | Version | Interval   | Last Download            | Next Download Check     |
|----------------|----------|---------|------------|--------------------------|-------------------------|
| iprep_et_rules | Checking | 1.1     | 4<br>hours | Wed Dec 31 23:59:00 2017 | Thu Jan 1 01:00:00 2018 |

The parameters in the example output are explained in the following table.

| Parameter           | Description   |
|---------------------|---|
| Resource Name       | Name of the updatable resource  |
| Status              | Resource status. There are five types of status: Sleeping, Checking, Starting, Downloading, Stopping. |
| Version             | Current version of the resource   |
| Interval            | Configured update check interval for the resource   |
| Last Download       | Time stamp of last resource downloaded  |
| Next Download Check | Time stamp of next download check for the resource  |

**Related commands** [update webgui now](#)

# update now

**Overview** Use this command to immediately perform a resource update check and update the specified resource if a newer version is available.

**Syntax** `update {<resource-name>|all} now`

| Parameter                          | Description  |
|------------------------------------|--|
| <code>&lt;resource-name&gt;</code> | Specific resource to update. You will get an error message if the resource does not exist. |
| <code>all</code>                   | Update all resources   |

**Mode** Privileged Exec

**Usage notes** The default update interval for a resource is 1 hour. Users can initiate an immediate update check for a resource at any time without affecting any configured update check schedule. The Update Manager will perform an update check for a resource when triggered to do so. The Update Manager will request the current version number of the resource from the Update Server, then compare it with the current local version. If they are different, the Update Manager will initiate an update of the local resource.

Note that if the feature is disabled, regular and manual update checks for its resources are also disabled.

Also note that an update check for a resource will not proceed if an update of that resource is already in progress.

The Update Manager will retry upon failure to download a resource file because of DNS resolution error, bad checksum and so on.

**Examples** To immediately do an update check and update if needed for all available resources, use the following command:

```
awplus#update all now
```

To immediately do an update check and update if needed for the IP Reputation feature, use the following command:

```
awplus#update iprep_et_rules now
```

**Related commands** [show resource](#)  
[update webgui now](#)

# update webgui now

**Overview** Use this command to check whether you have the latest version of the device's GUI and update it if a newer version is available.

**Syntax** `update webgui now`

**Mode** Privileged Exec

**Usage notes** This command applies since software version 5.4.6-1.1. Prior to 5.4.6-1.1, users used the **copy** command to copy GUI files onto the AR-series firewall instead. If you did that, you need to delete all GUI files from Flash memory before you run the "update webgui now" command. To delete all GUI files, use the command:

```
awplus#del *gui_*.tar.gz
```

**Examples** To check for GUI updates, use the following command:

```
awplus#update webgui now
```

**Related commands** [show resource](#)



# 6

# System Configuration and Monitoring Commands

## Introduction

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

- Command List**
- ["banner exec"](#) on page 171
  - ["banner login \(system\)"](#) on page 173
  - ["banner motd"](#) on page 175
  - ["clock set"](#) on page 177
  - ["clock summer-time date"](#) on page 178
  - ["clock summer-time recurring"](#) on page 180
  - ["clock timezone"](#) on page 182
  - ["debug core-file"](#) on page 183
  - ["hostname"](#) on page 184
  - ["max-fib-routes"](#) on page 186
  - ["max-static-routes"](#) on page 187
  - ["no debug all"](#) on page 188
  - ["reboot"](#) on page 190
  - ["receive-packet-scheduler"](#) on page 191
  - ["reload"](#) on page 193
  - ["show clock"](#) on page 194
  - ["show cpu"](#) on page 196
  - ["show cpu history"](#) on page 199
  - ["show debugging"](#) on page 201
  - ["show interface memory"](#) on page 202

- [“show memory”](#) on page 204
- [“show memory allocations”](#) on page 206
- [“show memory history”](#) on page 208
- [“show memory pools”](#) on page 209
- [“show memory shared”](#) on page 210
- [“show process”](#) on page 211
- [“show reboot history”](#) on page 213
- [“show router-id”](#) on page 214
- [“show system”](#) on page 215
- [“show system interrupts”](#) on page 216
- [“show system mac”](#) on page 217
- [“show system pci device”](#) on page 218
- [“show system pci tree”](#) on page 219
- [“show system serialnumber”](#) on page 220
- [“show tech-support”](#) on page 221
- [“speed \(asyn\)”](#) on page 223
- [“terminal monitor”](#) on page 225
- [“undebg all”](#) on page 226

# banner exec

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

**Syntax** banner exec <banner-text>  
banner exec default  
no banner exec

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

```
AlliedWare Plus (TM) 5.5.0 04/05/20 12:00:00
```

**Mode** Global Configuration

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

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

awplus login: manager
Password:

Use enable to move to Priv Exec mode

awplus>
```

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

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

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.0 04/05/20 12:00:00

awplus>
```

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

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

awplus login: manager
Password:

awplus>
```

**Related commands**

- [banner login \(system\)](#)
- [banner motd](#)

## banner login (system)

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

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

**Syntax** banner login  
no banner login

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

**Mode** Global Configuration

**Examples** To configure a login banner of “Authorized users only” to be displayed when you login, enter the following commands:

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

Authorized users only

awplus(config)#exit
awplus#exit

Authorized users only

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.0 04/05/20 12:00:00

awplus>
```

To remove the login banner, enter the following commands:

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

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.0 04/05/20 12:00:00

awplus>
```

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

# banner motd

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

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

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

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

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

**Mode** Global Configuration

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

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

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

AlliedWare Plus (TM) 5.5.0 04/05/20 12:00:00

awplus>
```

To delete the login banner, enter the following commands:

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

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.0 04/05/20 12:00:00

awplus>
```

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



# clock set

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

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

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

**Mode** Privileged Exec

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

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

**Example** To set the time and date on your system to 2pm on the 2nd of October 2016, use the command:

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

**Related commands** [clock timezone](#)

# clock summer-time date

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

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

By default, the device has no summertime definitions set.

**Syntax**

```
clock summer-time <timezone-name> date <start-day>
<start-month> <start-year> <start-time> <end-day> <end-month>
<end-year> <end-time> <1-180>

no clock summer-time
```

| Parameter       | Description   |
|-----------------|---|
| <timezone-name> | A description of the summertime zone, up to 6 characters long.                      |
| date            | Specifies that this is a date-based summertime setting for just the specified year. |
| <start-day>     | Day that the summertime starts, from 1 to 31.                                       |
| <start-month>   | First three letters of the name of the month that the summertime starts.            |
| <start-year>    | Year that summertime starts, from 2000 to 2035.                                     |
| <start-time>    | Time of the day that summertime starts, in the 24-hour time format HH:MM.           |
| <end-day>       | Day that summertime ends, from 1 to 31.   |
| <end-month>     | First three letters of the name of the month that the summertime ends.              |
| <end-year>      | Year that summertime ends, from 2000 to 2035.                                       |
| <end-time>      | Time of the day that summertime ends, in the 24-hour time format HH:MM.             |
| <1-180>         | The offset in minutes.  |

**Mode** Global Configuration

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

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

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

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

**Related commands** [clock summer-time recurring](#)  
[clock timezone](#)

# clock summer-time recurring

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

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

By default, the device has no summertime definitions set.

**Syntax**

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

no clock summer-time
```

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

**Mode** Global Configuration

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

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

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

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

**Related commands** [clock summer-time date](#)  
[clock timezone](#)

# clock timezone

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

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

By default, the system time is set to UTC.

**Syntax** `clock timezone <timezone-name> {minus|plus}`  
`[<0-13>|<0-12>:<00-59>]`

`no clock timezone`

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

**Mode** Global Configuration

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

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

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

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

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

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

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

**Related commands**

[clock set](#)

[clock summer-time date](#)

[clock summer-time recurring](#)

# debug core-file

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

**Syntax** debug core-file  
no debug core-file

**Default** Enabled.

**Mode** Global Configuration

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

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

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

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

**Command changes** Version 5.4.9-1.0: command added

# hostname

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

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

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

**Syntax** `hostname <hostname>`  
`no hostname [<hostname>]`

| Parameter                     | Description                                    |
|-------------------------------|--|
| <code>&lt;hostname&gt;</code> | Specifies the name given to a specific device. |

**Default** `awplus`

**Mode** Global Configuration

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

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

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

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

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

This changes the prompt to:

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

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

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

This changes the prompt to:

```
awplus(config)#
```



**NOTE:** When AMF is configured, running the **no hostname** command will apply a hostname that is based on the MAC address of the device node, for example, **node\_0000\_5e00\_5301**.

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

# max-fib-routes

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

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

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

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

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

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

**Mode** Global Configuration

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

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

# max-static-routes

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

**NOTE:** For FIB routes use the [max-fib-routes](#) command.

Use the **no** variant of this command to set the maximum number of static routes to the default of 1024 static routes.

**Syntax** `max-static-routes <1-1024>`  
`no max-static-routes`

**Default** The default number of static routes is the maximum number of static routes (1024).

**Mode** Global Configuration

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

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

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

**Related commands** [max-fib-routes](#)

# no debug all

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

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

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

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

**Default** The debugging facility is disabled by default.

**Mode** Global Configuration and Privileged Exec

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

```
awplus# no debug all
```

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
```

**Related commands** [undebug all](#)

**Command changes** Version 5.4.7-1.1: PIM Sparse Mode parameter added  
Version 5.4.7-1.1: RIP parameter added

# reboot

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

**Syntax** `reboot`  
`reload`

**Mode** Privileged Exec

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

**Examples** To restart the device, use the command:

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

# receive-packet-scheduler

**Overview** Use this command to configure a scheduling scheme that distributes packets to individual cores in a multi-core CPU.

Receive Packet Scheduling is the mechanism by which packets requiring software forwarding are distributed to individual cores in multi-core CPUs.

Use the **no** variant of this command to set the scheduling scheme back to the default of hash.

**Syntax** `receive-packet-scheduler {hash|balanced|split}`  
`no receive-packet-scheduler`

| Parameter | Description  |
|-----------|--|
| hash      | Hardware 5-Tuple flow hash-based packet core scheduling. This is the most suitable scheduling scheme for all scenarios.  |
| balanced  | Packets are balanced across cores as efficiently as possible providing the best performance for single flow scenarios.   |
| split     | Half of the CPU cores in a multi-core device are reserved for packet processing. These cores process packets using the default hash-based scheme. The other half of the processing cores are reserved for the IPsec encryption/decryption process. |

**Default** Hash.

**Mode** Global Configuration

**Usage notes** Receive Packet Scheduling is the mechanism by which packets requiring software forwarding are distributed to individual cores in multi-core CPUs.

AlliedWare Plus uses a flow hash based scheme to ensure packets from the same flow are processed in order on the same core. This is generally accepted as the best compromise between efficiency and stability for most network traffic.

There are however a few scenarios where a different mechanism may be required. Use this command to configure alternative packet scheduling algorithms to suit your traffic patterns.

**NOTE:** *It is very unlikely that there would be any need to change from the default receive-packet-scheduling scheme (hash) as it is the most suitable mechanism for real network traffic.*

**CAUTION:** *Changing the receive packet scheduling may require IPsec SA's to be processed on a different CPU core. Hence if there are active IPsec SA's when the scheme is changed they may no longer operate correctly. All active SA's can be reset using the **clear isakmp sa** command.*

**Example** To configure the receive packet scheduling scheme to **split**, use the following commands:

```
awplus# configure terminal
awplus(config)# receive-packet-scheduler split
```

To set the receive packet scheduling back to the default of **hash**, use the following commands:

```
awplus# configure terminal
awplus(config)# no receive-packet-scheduler
```

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

**Command changes** Version 5.4.8-2.1: command added



# 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 6-1: Example output from the **show clock** command for a device using New Zealand time

```
Local Time: Mon, 17 Oct 2016 13:56:06 +1200
UTC Time: Mon, 17 Oct 2016 01:56:06 +0000
Timezone: NZST
Timezone Offset: +12:00
Summer time zone: NZDT
Summer time starts: Last Sunday in September at 02:00:00
Summer time ends: First Sunday in April at 02:00:00
Summer time offset: 60 mins
Summer time recurring: Yes
```

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

| Parameter             | Description   |
|-----------------------|---|
| Local Time            | Current local time.   |
| UTC Time              | Current UTC time.   |
| Timezone              | The current configured timezone name.   |
| Timezone Offset       | Number of hours offset to UTC.  |
| Summer time zone      | The current configured summertime zone name.                                    |
| Summer time starts    | Date and time set as the start of summer time.                                  |
| Summer time ends      | Date and time set as the end of summer time.                                    |
| Summer time offset    | Number of minutes that summer time is offset from the system's timezone.        |
| Summer time recurring | Whether the device will apply the summer time settings every year or only once. |

**Related commands**

- [clock set](#)
- [clock summer-time date](#)
- [clock summer-time recurring](#)
- [clock timezone](#)

# show cpu

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

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

**Syntax** `show cpu [sort {thrds|pri|sleep|runtime}]`

| Parameter | Description   |
|-----------|---|
| sort      | Changes the sorting order using the following fields. If you do not specify a field, then the list is sorted by percentage CPU utilization. |
| thrds     | Sort by the number of threads.  |
| pri       | Sort by the process priority.   |
| sleep     | Sort by the average time sleeping.  |
| runtime   | Sort by the runtime of the process.   |

**Mode** User Exec and Privileged Exec

**Examples** To show the CPU utilization of current processes, sorting them by the number of threads the processes are using, use the command:

```
awplus# show cpu sort thrds
```

**Output** Figure 6-2: Example output from **show cpu**

```
awplus#show cpu
CPU averages:
 1 second: 0%, 20 seconds: 0%, 60 seconds: 0%
System load averages:
 1 minute: 0.16, 5 minutes: 0.13, 15 minutes: 0.13
Current CPU load:
 userspace: 2%, kernel: 6%, interrupts: 0% iowaits: 0%

user processes
=====
 pid name          thrds  cpu%   pri state sleep% runtime
763 hostd          1    2.9   20  run   0    128
803 diag_monitor  1    0.4   20  sleep 0   3292
768 hsl           14    0.4   20  sleep 0   3912
 1 init           1    0.0   20  sleep 0    686
478 rtccludge     1    0.0   20  sleep 0     9
504 portmap       1    0.0   20  sleep 0     2
17555 sh          1    0.0   20  sleep 0     1
17556 console_log_ale 1    0.0   20  sleep 0     1
 515 syslog-ng    1    0.0   20  sleep 0    153
 521 dbus-daemon  1    0.0   20  sleep 0     2
 532 automount    1    0.0   20  sleep 0    453
 571 appmond      1    0.0   20  sleep 0     41
 587 crond        1    0.0   20  sleep 0     17
 589 openhpid     9    0.0   20  sleep 0    284
 609 inetd        1    0.0   20  sleep 0     2
 761 nsm           1    0.0   20  sleep 0    260
 765 imi          1    0.0   20  sleep 0    616
 799 almond       1    0.0   20  sleep 0     52
 805 cntrd        1    0.0   20  sleep 0     45
 807 poehw        3    0.0   20  sleep 0    207
 820 authd        1    0.0   20  sleep 0     76
...

kernel threads
=====
 pid name          cpu%   pri state sleep% runtime
144 aio            0.0    0  sleep  0     0
 95 bdi-default    0.0   20  sleep  0     0
149 crypto         0.0    0  sleep  0     0
474 flush-31:4    0.0   20  sleep  0     1
143 fsnotify_mark 0.0   20  sleep  0     0
426 jffs2_gcd_mtd0 0.0   30  sleep  0   353
 96 kblockd       0.0    0  sleep  0     0
 12 khelper       0.0    0  sleep  0     0
105 khubd         0.0   20  sleep  0     0
 3 ksoftirqd/0    0.0   20  sleep  0     0
142 kswapd0       0.0   20  sleep  0     0
 2 kthreadd       0.0   20  sleep  0     0
 4 kworker/0:0    0.0   20  sleep  0    29
 6 linkwatch     0.0    0  sleep  0     0
466 loop0        0.0    0  sleep  0   801
 7 migration/0    0.0  -100  sleep  0     0
244 mtddblock0    0.0   20  sleep  0     5
 93 sync_supers   0.0   20  sleep  0     1
```

**Table 2:** Parameters in the output of the **show cpu** command

| Parameter            | Description   |
|----------------------|---|
| CPU averages         | Average CPU utilization for the periods stated.   |
| System load averages | The average number of processes waiting for CPU time for the periods stated.  |
| Current CPU load     | Current CPU utilization specified by load types.  |
| pid                  | Identifier number of the process.   |
| name                 | A shortened name for the process  |
| thrds                | Number of threads in the process.   |
| cpu%                 | Percentage of CPU utilization that this process is consuming.   |
| pri                  | Process priority state.   |
| state                | Process state; one of "run", "sleep", "zombie", and "dead".   |
| sleep%               | Percentage of time that the process is in the sleep state.  |
| runtime              | The time that the process has been running for, measured in jiffies. A jiffy is the duration of one tick of the system timer interrupt. |

- Related commands**
- [show memory](#)
  - [show memory allocations](#)
  - [show memory history](#)
  - [show memory pools](#)
  - [show process](#)

# show cpu history

**Overview** This command prints a graph showing the historical CPU utilization. For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show cpu history`

**Mode** User Exec and Privileged Exec

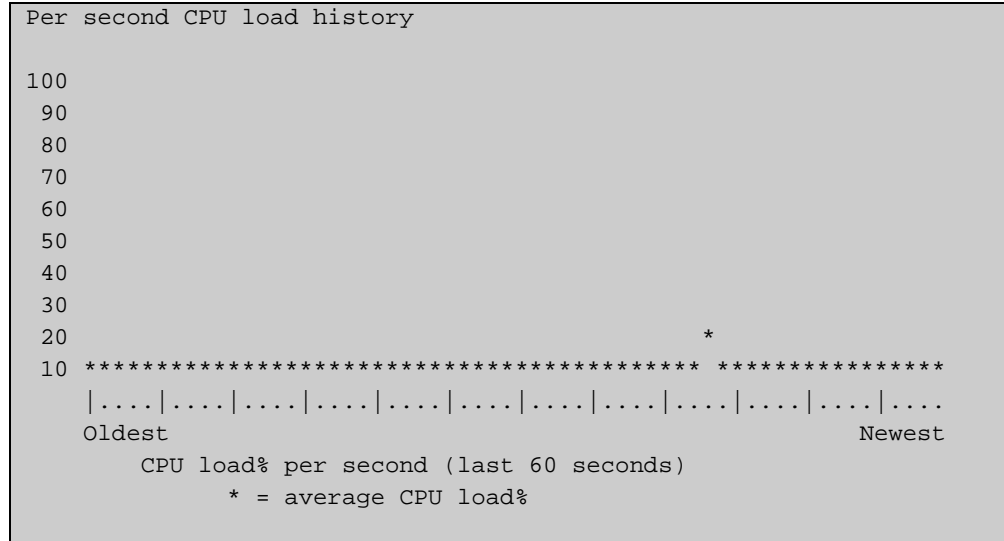
**Usage notes** This command’s output displays three graphs of the percentage CPU utilization:

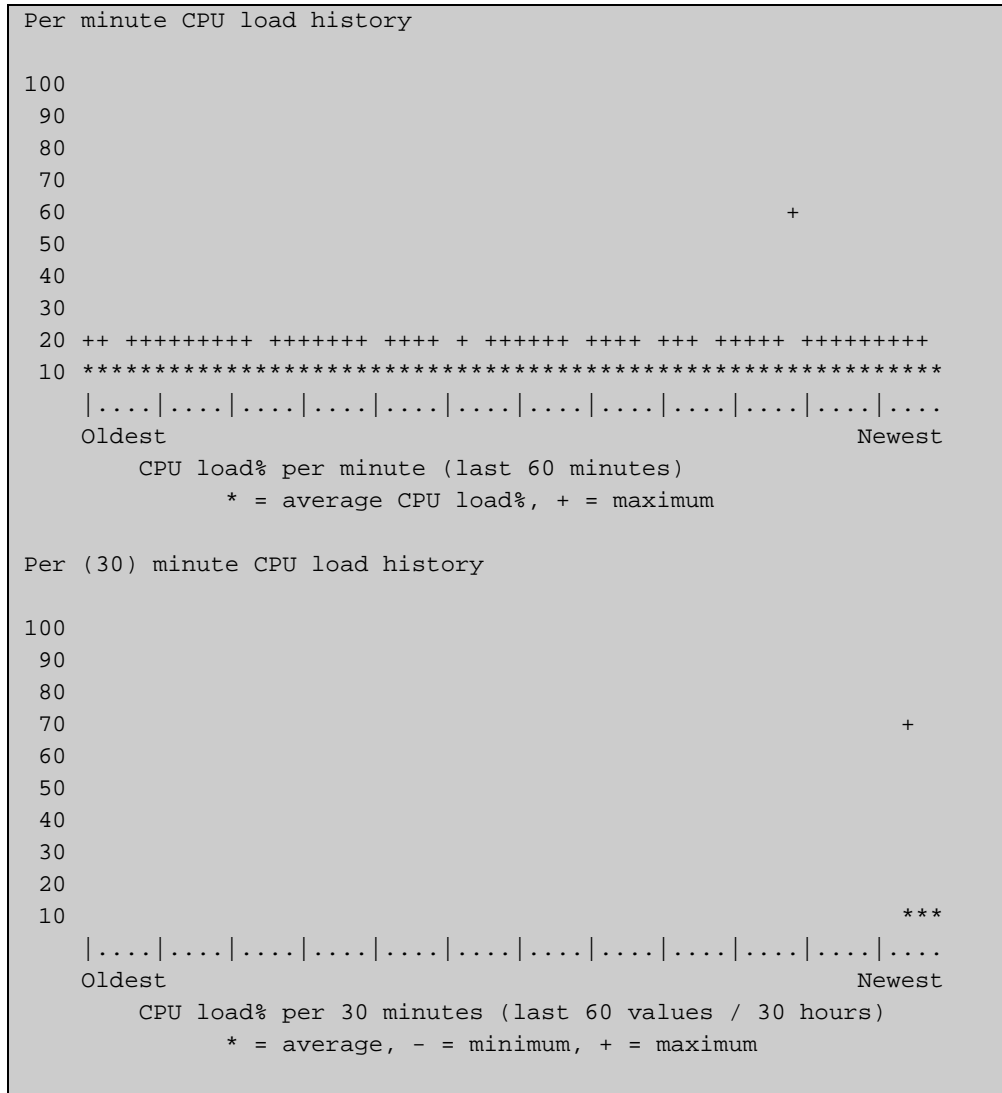
- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

**Examples** To display a graph showing the historical CPU utilization of the device, use the command:

```
awplus# show cpu history
```

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





- Related commands**
- [show memory](#)
  - [show memory allocations](#)
  - [show memory pools](#)
  - [show process](#)



# show debugging

**Overview** This command displays all debugging options in alphabetical order, indicating whether debugging is enabled or disabled for each feature.

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

**Syntax** show debugging

**Mode** User Exec and Privileged Exec

**Example** To find out what debugging is enabled, use the command:

```
awplus# show debugging
```

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

```
awplus#show debugging
ATMF debugging status:
ATMF arealink debugging is off
ATMF link debugging is off
...
DDNS debugging status:
  DDNS debugging is off
Firewall Debugging Status: off
DNS Relay debugging status:
  debugging is off
IP packet debugging status:
ISAKMP Debugging status:
  CFG (Configuration management)           disabled
  CHD (Child SA/IPsec SA)                  disabled
  DMN (Main daemon signal handling)        disabled
  ENC (Packet encryption/decryption)       disabled
  IKE (IKE SA/ISAKMP SA)                   disabled
...
NSM debugging status:

Platform packet debugging is off

PPP debugging status:

Snmp (AgentX: Operational state, sock 78) debugging status:
  Snmp debugging is off
Trigger debugging status:
  Trigger debugging is off
```

# show interface memory

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

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

**Syntax** `show interface memory`  
`show interface <port-list> memory`

| Parameter   | Description   |
|-------------|---|
| <port-list> | Display information about only the specified port or ports. The port list can be: <ul style="list-style-type: none"><li>• an Eth port (e.g. eth1)</li><li>• a switchport (e.g. port1.0.4)</li><li>• a continuous range of ports separated by a hyphen (e.g. port1.0.1-1.0.4)</li><li>• a comma-separated list (e.g. port1.0.1,port1.0.3-1.0.4). Do not mix port types in the same list.</li></ul> |

**Mode** User Exec and Privileged Exec

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

```
awplus# show interface memory
```

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

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

**Output** Figure 6-5: Example output from the **show interface memory** command

```
awplus#show interface memory
Vlan blocking state shared memory usage
-----
Interface    shmid      Bytes Used  natch    Status
port1.0.1    294921     512         1
port1.0.2    491535     512         1
port1.0.3    458766     512         1
...
eth1         393228     512         1
lo           360459     512         1
```

Figure 6-6: Example output from **show interface <port-list> memory** for a list of interfaces

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

**Related  
commands**

- [show interface brief](#)
- [show interface status](#)
- [show interface switchport](#)

# show memory

**Overview** This command displays the memory used by each process that is currently running. For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

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

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

**Mode** User Exec and Privileged Exec

**Example** To display the memory used by the current running processes, use the command:  
`awplus# show memory`

**Output** Figure 6-7: Example output from **show memory**

```
awplus#show memory

RAM total: 824680 kB; free: 635032 kB; buffers: 20272 kB

user processes
=====
 pid name          mem%  size(kB)  peak(kB)  data(kB)  stk(kB)  virt(kB)
1443 squid          1.9    16408    299768    23568     264     299768
1441 squid          1.9    16416    299776    23568     272     299776
1440 squid          1.9    16416    299776    23568     272     299776
1439 squid          1.9    16416    299776    23568     272     299776
1438 squid          1.9    16152    298928    23568     264     298864
1226 imi            1.3    10968     23104     2760      160      22912
1228 hsl            1.2    10512    692944    608160    144     631856
2156 imish          1.0     8856    158456    75904     160     94696
1221 nsm            1.0     9008     21696     1968      152     21632
1296 ospfd          0.8     6936     19144     1016      144     19080
1293 bgpd           0.8     7264     19184     1168      152     19120
1291 pimd           0.8     6600     20992     2944      144     20928
1283 ripd           0.8     6640     18328     944       152     18256
...
```

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

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

**Related commands**

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

# show memory allocations

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

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

**Syntax** show memory allocations [<process>]

| Parameter | Description   |
|-----------|---|
| <process> | Displays the memory allocation used by the specified process. |

**Mode** User Exec and Privileged Exec

**Example** To display the memory allocations used by all processes on your device, use the command:

```
awplus# show memory allocations
```

**Output** Figure 6-8: Example output from the **show memory allocations** command

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

Current 15093760 (peak 15093760)

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

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

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

**Related commands**

- show memory
- show memory history
- show memory pools
- show memory shared
- show tech-support

# show memory history

**Overview** This command prints a graph showing the historical memory usage.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show memory history`

**Mode** User Exec and Privileged Exec

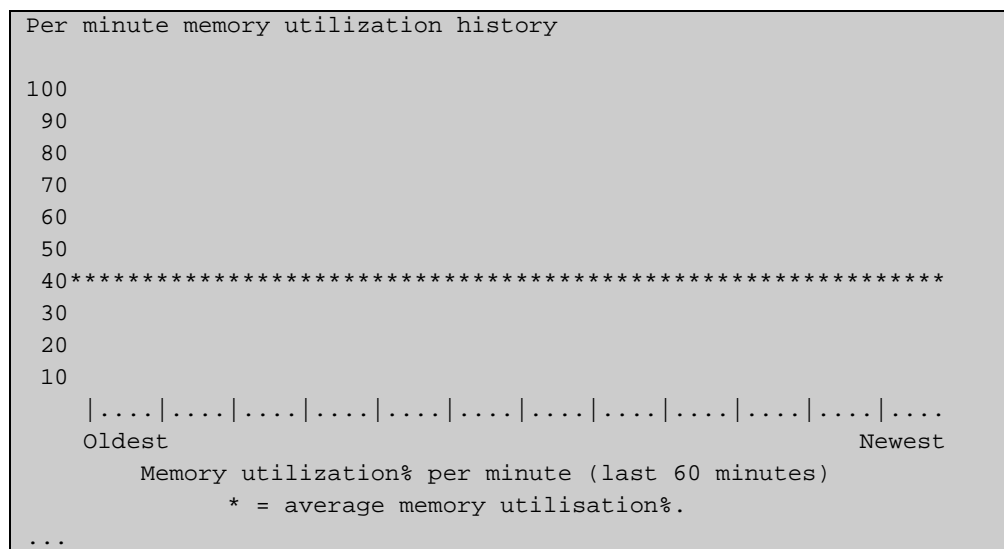
**Usage notes** This command’s output displays three graphs of the percentage memory utilization:

- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

**Examples** To show a graph displaying the historical memory usage, use the command:

```
awplus# show memory history
```

**Output** Figure 6-9: Example output from the **show memory history** command



- Related commands**
- [show memory allocations](#)
  - [show memory pools](#)
  - [show memory shared](#)
  - [show tech-support](#)



# show memory pools

**Overview** This command shows the memory pools used by processes.

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

**Syntax** `show memory pools [<process>]`

| Parameter                    | Description  |
|------------------------------|--|
| <code>&lt;process&gt;</code> | Displays the memory pools used by the specified process. |

**Mode** User Exec and Privileged Exec

**Example** To show the memory pools used by processes, use the command:

```
awplus# show memory pools
```

**Output** Figure 6-10: Example output from the **show memory pools** command

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

Current 15290368 (peak 15290368)

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

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

**Related commands**

- [show memory allocations](#)
- [show memory history](#)
- [show tech-support](#)

# show memory shared

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

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

**Syntax** `show memory shared`

**Mode** User Exec and Privileged Exec

**Example** To display information about the shared memory allocation used on the device, use the command:

```
awplus# show memory shared
```

**Output** Figure 6-11: Example output from the **show memory shared** command

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

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

**Related commands**

- [show memory allocations](#)
- [show memory history](#)
- [show memory](#)

# show process

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

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

**Syntax** `show process [sort {cpu|mem}]`

| Parameter | Description   |
|-----------|---|
| sort      | Changes the sorting order for the list of processes.    |
| cpu       | Sorts the list by the percentage of CPU utilization.    |
| mem       | Sorts the list by the percentage of memory utilization. |

**Mode** User Exec and Privileged Exec

**Usage notes** This command displays a snapshot of currently-running processes. If you want to see CPU or memory utilization history instead, use the commands [show cpu history](#) or [show memory history](#).

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

```
awplus# show process
```

**Output** Figure 6-12: Example output from the **show process** command

```
CPU averages:
 1 second: 8%, 20 seconds: 5%, 60 seconds: 5%
System load averages:
 1 minute: 0.04, 5 minutes: 0.08, 15 minutes: 0.12
Current CPU load:
 userspace: 9%, kernel: 9%, interrupts: 0% iowaits: 0%
RAM total: 514920 kB; free: 382600 kB; buffers: 16368 kB

user processes
=====
pid name      thrds  cpu%  mem%  pri  state  sleep%
962 pss        12    0     6    25  sleep    5
1  init         1     0     0    25  sleep    0
797 syslog-ng   1     0     0    16  sleep   88
...
kernel threads
=====
pid name      cpu%  pri  state  sleep%
71  aio/0      0    20  sleep  0
3   events/0   0    10  sleep  98
...
```

**Table 4:** Parameters in the output from the **show process** command

| Parameter            | Description  |
|----------------------|--|
| CPU averages         | Average CPU utilization for the periods stated.                              |
| System load averages | The average number of processes waiting for CPU time for the periods stated. |
| Current CPU load     | Current CPU utilization specified by load types                              |
| RAM total            | Total memory size.   |
| free                 | Available memory.  |
| buffers              | Memory allocated to kernel buffers.  |
| pid                  | Identifier for the process.  |
| name                 | Short name to describe the process.  |
| thrds                | Number of threads in the process.  |
| cpu%                 | Percentage of CPU utilization that this process is consuming.                |
| mem%                 | Percentage of memory utilization that this process is consuming.             |
| pri                  | Process priority.  |
| state                | Process state; one of "run", "sleep", "stop", "zombie", or "dead".           |
| sleep%               | Percentage of time the process is in the sleep state.                        |

**Related commands** [show cpu](#)  
[show cpu history](#)

# show reboot history

**Overview** Use this command to display the device's reboot history.

**Syntax** show reboot history

**Mode** User Exec and Privileged Exec

**Example** To show the reboot history, use the command:

```
awplus# show reboot history
```

**Output** Figure 6-13: Example output from the **show reboot history** command

```
awplus#show reboot history

<date>      <time>      <type>      <description>
-----
2016-10-10  01:42:04  Expected    User Request
2016-10-10  01:35:31  Expected    User Request
2016-10-10  01:16:25  Unexpected  Rebooting due to critical process (network/nsm)
failure!
2016-10-10  01:11:04  Unexpected  Rebooting due to critical process (network/nsm)
failure!
2016-10-09  19:56:16  Expected    User Request
2016-10-09  19:51:20  Expected    User Request
```

**Table 5:** Parameters in the output from the **show reboot history** command

| Parameter    | Description                         |
|--------------|-------------------------------------|
| Unexpected   | A non-intended reboot.              |
| Expected     | A planned or user-triggered reboot. |
| User request | User initiated reboot via the CLI.  |

**Related commands** [show tech-support](#)

# show router-id

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

**Syntax** `show router-id`

**Mode** User Exec and Privileged Exec

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

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

**Output** Figure 6-14: 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, memory usage, and software version. It also displays location and contact details when these have been set.

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

**Syntax** `show system`

**Mode** User Exec and Privileged Exec

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

```
awplus# show system
```

**Output** Figure 6-15: Example output from **show system**

```
awplus#show system
System Status                               Mon Jul 22 14:02:21 2019

Board      ID   Bay   Board Name          Rev   Serial number
-----
Base       560 Base   AR1050V             A-0   0000000000000034
-----

RAM: Total: 432760 kB Free: 279336 kB
Flash: 106.4MB Used: 69.9MB Available: 36.5MB
-----

Uptime           : 0 days 00:07:59
Bootloader version : 5.2.0

Current software  : AR1050V-5.4.9-0.1.rel
Software version  : 5.4.9-0.1
Build date       : Fri Mar 29 15:03:33 UTC 2019

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

System Name
awplus
System Contact

System Location
-----
```

# show system interrupts

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

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

**Syntax** `show system interrupts`

**Mode** User Exec and Privileged Exec

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

```
awplus# show system interrupts
```

**Output** Figure 6-16: Example output from the **show system interrupts** command

```
awplus#show system interrupts
      CPU0      CPU1
8:    151378    152020    Core Enabled  0 timer
16:      0      0      CIU Enabled  0 Ethernet
25:     256      0      CIU-W Enabled  0 octeon_wdt
26:      0     256      CIU-W Enabled  0 octeon_wdt
41:   946096   947120      CIU-M Enabled  0 SMP-IPI
51:      0      0      CIU Enabled  0 RGMII
53:      0      0      CIU Enabled  0 Ethernet
59:    1025      0      CIU Enabled  0 serial
60:    5825      0      CIU Enabled  0 i2c-octeon
61:      3      0      CIU Enabled  0 i2c-octeon
63:      0      0      CIB Enabled  0 xhci-hcd:usb1
65:      0      0      CIU-GPIO Enabled  0 0-0021
...
```



# show system mac

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

**Syntax** `show system mac`

**Mode** User Exec and Privileged Exec

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

```
awplus# show system mac
```

**Output** Figure 6-17: Example output from the **show system mac** command

```
awplus#show system mac
0200.0034.5682
0200.0034.5683
0200.0034.5684
```

# 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

```
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 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
```

**Related commands** [show system pci device](#)

# show system serialnumber

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

**Syntax** `show system serialnumber`

**Mode** User Exec and Privileged Exec

**Example** To display the serial number information for the device, use the command:

```
awplus# show system serialnumber
```

**Output** Figure 6-18: 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.

This command is useful for collecting a large amount of information so that it can then be analyzed for troubleshooting purposes. The output of this command can be provided to technical support staff when reporting a problem.

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

**Syntax** `show tech-support`  
{[all|atmf|auth|bgp|card|dhcpcsn|epsr|firewall|igmp|ip|ipv6|mld|openflow|ospf|ospf6|pim|rip|ripng|stack|stp|system|tacacs+|update]} [outfile <filename>]

| Parameter | Description                                |
|-----------|--|
| all       | Display full information                   |
| atmf      | Display ATMF-specific information          |
| auth      | Display authentication-related information |
| bgp       | Display BGP-related information            |
| card      | Display Chassis Card specific information  |
| dhcpcsn   | Display DHCP Snooping specific information |
| epsr      | Display EPSR specific information          |
| firewall  | Display firewall specific information      |
| igmp      | Display IGMP specific information          |
| ip        | Display IP specific information            |
| ipv6      | Display IPv6 specific information          |
| mld       | Display MLD specific information           |
| openflow  | Display information related to OpenFlow    |
| ospf      | Display OSPF related information           |
| ospf6     | Display OSPF6 specific information         |
| pim       | Display PIM related information            |
| rip       | RIP related information                    |
| ripng     | Display RIPNG specific information         |
| stack     | Display stacking device information        |
| stp       | Display STP specific information           |
| system    | Display general system information         |

| Parameter  | Description   |
|------------|---|
| tacacs+    | Display TACACS+ information   |
| update     | Display resource update specific information  |
|            | Output modifier   |
| >          | Output redirection  |
| >>         | Output redirection (append)   |
| outfile    | Output file name  |
| <filename> | Specifies a name for the output file. If no name is specified, this file will be saved as: tech-support.txt.gz. |

**Default** Captures **all** information for the device.

By default the output is saved to the file 'tech-support.txt.gz' in the current directory. If this file already exists in the current directory then a new file is generated with the time stamp appended to the file name, for example 'tech-support20161009.txt.gz', so the previous file is retained.

**Usage notes** The command generates a large amount of output, which is saved to a file in compressed format. The output file name can be specified by outfile option. If the output file already exists, a new file name is generated with the current time stamp. If the output filename does not end with ".gz", then ".gz" is appended to the filename. Since output files may be too large for Flash on the device we recommend saving files to external memory or a TFTP server whenever possible to avoid device lockup. This method is not likely to be appropriate when running the working set option of AMF across a range of physically separated devices.

**Mode** Privileged Exec

**Examples** To produce the output needed by technical support staff, use the command:

```
awplus# show tech-support
```

# speed (asyn)

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

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

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

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

**Mode** Line Configuration

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

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

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

Then log in again to enable the change:

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

**Related commands**

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



# terminal monitor

**Overview** Use this command to display debugging output on a terminal.  
To display the cursor after a line of debugging output, press the Enter key.  
Use the command **terminal no monitor** or **no terminal monitor** to stop displaying debugging output on the terminal. Alternatively, you can use the timeout option to stop displaying debugging output on the terminal after a set time.

**Syntax** terminal monitor [<1-60>]  
terminal no monitor  
no terminal monitor

| Parameter | Description   |
|-----------|---|
| <1-60>    | Set a timeout between 1 and 60 seconds for terminal output. |

**Default** Disabled

**Mode** User Exec and Privileged Exec

**Examples** To display debugging output on a terminal, enter the command:

```
awplus# terminal monitor
```

To display debugging on the terminal for 60 seconds, enter the command:

```
awplus# terminal monitor 60
```

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

```
awplus# no terminal monitor
```

**Related commands** All debug commands

**Command changes** Version 5.4.8-0.2: **no terminal monitor** added as an alias for **terminal no monitor**

# undebug all

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

# 7

# Logging Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure logging. See the [Logging Feature Overview and Configuration Guide](#) for more information about the different types of log and how to filter log messages.

- Command List**
- [“clear exception log”](#) on page 230
  - [“clear log”](#) on page 231
  - [“clear log buffered”](#) on page 232
  - [“clear log external”](#) on page 233
  - [“clear log permanent”](#) on page 234
  - [“connection-log events”](#) on page 235
  - [“copy buffered-log”](#) on page 236
  - [“copy permanent-log”](#) on page 237
  - [“default log buffered”](#) on page 238
  - [“default log console”](#) on page 239
  - [“default log email”](#) on page 240
  - [“default log external”](#) on page 241
  - [“default log host”](#) on page 242
  - [“default log monitor”](#) on page 243
  - [“default log permanent”](#) on page 244
  - [“log buffered”](#) on page 245
  - [“log buffered \(filter\)”](#) on page 246
  - [“log buffered exclude”](#) on page 249
  - [“log buffered size”](#) on page 252

- [“log console”](#) on page 253
- [“log console \(filter\)”](#) on page 254
- [“log console exclude”](#) on page 257
- [“log date-format”](#) on page 260
- [“log email”](#) on page 261
- [“log email \(filter\)”](#) on page 262
- [“log email exclude”](#) on page 265
- [“log email time”](#) on page 268
- [“log external”](#) on page 270
- [“log external \(filter\)”](#) on page 272
- [“log external exclude”](#) on page 275
- [“log external rotate”](#) on page 278
- [“log external size”](#) on page 280
- [“log facility”](#) on page 281
- [“log host”](#) on page 283
- [“log host \(filter\)”](#) on page 285
- [“log host exclude”](#) on page 288
- [“log host source”](#) on page 291
- [“log host startup-delay”](#) on page 292
- [“log host time”](#) on page 294
- [“log monitor \(filter\)”](#) on page 296
- [“log monitor exclude”](#) on page 299
- [“log permanent”](#) on page 302
- [“log permanent \(filter\)”](#) on page 303
- [“log permanent exclude”](#) on page 306
- [“log permanent size”](#) on page 309
- [“log-rate-limit nsm”](#) on page 310
- [“log trustpoint”](#) on page 311
- [“log url-requests”](#) on page 312
- [“show connection-log events”](#) on page 313
- [“show counter log”](#) on page 314
- [“show exception log”](#) on page 315
- [“show log”](#) on page 316
- [“show log config”](#) on page 318
- [“show log external”](#) on page 320

- [“show log permanent”](#) on page 321
- [“show running-config log”](#) on page 322
- [“unmount”](#) on page 323

# clear exception log

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

**Syntax** `clear exception log`

**Mode** Privileged Exec

**Example** `awplus# clear exception log`

# clear log

**Overview** This command removes the contents of the buffered and permanent logs.

**Syntax** `clear log`

**Mode** Privileged Exec

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

```
awplus# clear log
```

**Related commands**

- [clear log buffered](#)
- [clear log permanent](#)
- [show log](#)

# clear log buffered

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

**Syntax** `clear log buffered`

**Mode** Privileged Exec

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

```
awplus# clear log buffered
```

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

[log buffered](#)

[log buffered \(filter\)](#)

[log buffered size](#)

[log buffered exclude](#)

[show log](#)

[show log config](#)



# clear log external

**Overview** Use this command to delete the external log file from the USB storage device it is stored on.

If the external log is rotating between multiple files, this command deletes all those files, not just the most recent one.

**Syntax** `clear log external`

**Mode** Privileged Exec

**Example** To delete the external log file, use the command:

```
awplus# clear log external
```

**Related commands**

- [default log external](#)
- [log external](#)
- [log external \(filter\)](#)
- [log external exclude](#)
- [log external rotate](#)
- [log external size](#)
- [show log config](#)
- [show log external](#)
- [unmount](#)

**Command changes** Version 5.4.7-1.1: command added

# clear log permanent

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

**Syntax** clear log permanent

**Mode** Privileged Exec

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

```
awplus# clear log permanent
```

**Related commands**

- default log permanent
- log permanent
- log permanent (filter)
- log permanent exclude
- log permanent size
- show log config
- show log permanent

# connection-log events

**Overview** Use this command to enable extra logging for indicating the start and the end of connections passing through the firewall.

Use the **no** variant of this command to turn off the extra logging of connections passing through the firewall.

**Syntax** `connection-log events [new|end|all]`  
`no connection-log events [new|end|all]`

| Parameter | Description  |
|-----------|--|
| new       | New connection                                       |
| end       | Connections closed                                   |
| all       | All new connections and connections closed. Default. |

**Default** Connection logging is not enabled by default.

**Mode** Global Configuration.

**Usage notes** There are two types of messages you can log: new connections and connections that ended. You can control the amount of messages you log by choosing to log either type of message or all of the message types.

Messages contain the following information:

- time
- source and destination addresses (NATed and unNATed)
- protocol
- source and destination ports (NATed and unNATed)
- bytes and packets passed (found in the connection end message)

**Example** To log all of the new connections and all of the closed connections, use the commands:

```
awplus# configure terminal
awplus(config)# connection-log events all
```

**Related commands** [show connection-log events](#)

**Command changes** Version 5.4.7-1.1: command added.

# copy buffered-log

**Overview** Use this command to copy the buffered log to an internal or external destination.

**Syntax** `copy buffered-log <destination-name>`

| Parameter                             | Description   |
|---------------------------------------|---|
| <code>&lt;destination-name&gt;</code> | The filename and path for the destination file. See <a href="#">Introduction</a> on page 61 for valid syntax. |

**Mode** Privileged Exec

**Example** To copy the buffered log file into a folder in Flash named "buffered-log" and name the file "buffered-log.log", use the command:

```
awplus# copy buffered-log flash:/buffered-log/buffered-log.log
```

To copy the buffered log file onto a USB storage device and name the file "buffered-log.log", use the command:

```
awplus# copy buffered-log usb:/buffered-log.log
```

**Related commands** [log buffered](#)

[show file systems](#)

[show log](#)

**Command changes** Version 5.4.7-1.1: command added

# copy permanent-log

**Overview** Use this command to copy the permanent log to an internal or external destination.

**Syntax** `copy permanent-log <destination-name>`

| Parameter                             | Description   |
|---------------------------------------|---|
| <code>&lt;destination-name&gt;</code> | The filename and path for the destination file. See <a href="#">Introduction</a> on page 61 for valid syntax. |

**Mode** Privileged Exec

**Example** To copy the permanent log file into a folder in Flash named “perm-log” and name the file “permanent-log.log”, use the command:

```
awplus# copy permanent-log flash:/perm-log/permanent-log.log
```

To copy the permanent log file onto a USB storage device and name the file “permanent-log.log”, use the command:

```
awplus# copy permanent-log usb:/permanent-log.log
```

**Related commands**

- [log permanent](#)
- [show file systems](#)
- [show log permanent](#)

**Command changes** Version 5.4.7-1.1: command added

# default log buffered

**Overview** This command restores the default settings for the buffered log stored in RAM. By default the size of the buffered log is 50 kB and it accepts messages with the severity level of “warnings” and above.

**Syntax** `default log buffered`

**Default** The buffered log is enabled by default.

**Mode** Global Configuration

**Example** To restore the buffered log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log buffered
```

**Related commands**

- [clear log buffered](#)
- [log buffered](#)
- [log buffered \(filter\)](#)
- [log buffered size](#)
- [log buffered exclude](#)
- [show log](#)
- [show log config](#)

# default log console

**Overview** This command restores the default settings for log messages sent to the terminal when a `log console` command is issued. By default all messages are sent to the console when a `log console` command is issued.

**Syntax** `default log console`

**Mode** Global Configuration

**Example** To restore the log console to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log console
```

**Related commands**

- `log console`
- `log console (filter)`
- `log console exclude`
- `show log config`

# default log email

**Overview** This command restores the default settings for log messages sent to an email address. By default no filters are defined for email addresses. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

**Syntax** `default log email <email-address>`

| Parameter                          | Description                               |
|------------------------------------|---|
| <code>&lt;email-address&gt;</code> | The email address to send log messages to |

**Mode** Global Configuration

**Example** To restore the default settings for log messages sent to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# default log email admin@alliedtelesis.com
```

**Related commands**

- [log email](#)
- [log email \(filter\)](#)
- [log email exclude](#)
- [log email time](#)
- [show log config](#)



# default log external

**Overview** Use this command to restore the default settings for the external log. By default, the size of the external log is 50 kB, it rotates through 1 additional file, and it accepts messages with a severity level of notices and above.

Note that this command does not clear the configured filename for the external log.

**Syntax** `default log external`

**Mode** Global Configuration

**Example** To restore the default settings for the external log, use the commands:

```
awplus# configure terminal
awplus(config)# default log external
```

**Related commands**

- [clear log external](#)
- [log external](#)
- [log external \(filter\)](#)
- [log external exclude](#)
- [log external rotate](#)
- [log external size](#)
- [show log config](#)
- [show log external](#)
- [unmount](#)

**Command changes** Version 5.4.7-1.1: command added

# default log host

**Overview** This command restores the default settings for log sent to a remote syslog server. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

**Syntax** `default log host <ip-addr>`

| Parameter                    | Description                              |
|------------------------------|--|
| <code>&lt;ip-addr&gt;</code> | The IP address of a remote syslog server |

**Mode** Global Configuration

**Example** To restore the default settings for messages sent to the remote syslog server with IP address 10.32.16.21 use the following commands:

```
awplus# configure terminal
awplus(config)# default log host 10.32.16.21
```

**Related commands**

- [log host](#)
- [log host \(filter\)](#)
- [log host exclude](#)
- [log host source](#)
- [log host time](#)
- [show log config](#)

# default log monitor

**Overview** This command restores the default settings for log messages sent to the terminal when a [terminal monitor](#) command is used.

**Syntax** `default log monitor`

**Default** All messages are sent to the terminal when a [terminal monitor](#) command is used.

**Mode** Global Configuration

**Example** To restore the log monitor to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log monitor
```

**Related commands**

- [log monitor \(filter\)](#)
- [log monitor exclude](#)
- [show log config](#)
- [terminal monitor](#)

# default log permanent

**Overview** This command restores the default settings for the permanent log stored in NVS. By default, the size of the permanent log is 50 kB and it accepts messages with the severity level of warnings and above.

**Syntax** `default log permanent`

**Default** The permanent log is enabled by default.

**Mode** Global Configuration

**Example** To restore the permanent log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log permanent
```

**Related commands**

- [clear log permanent](#)
- [log permanent](#)
- [log permanent \(filter\)](#)
- [log permanent exclude](#)
- [log permanent size](#)
- [show log config](#)
- [show log permanent](#)

# log buffered

**Overview** This command configures the device to store log messages in RAM. Messages stored in RAM are not retained on the device over a restart. Once the buffered log reaches its configured maximum allowable size old messages will be deleted to make way for new ones.

**Syntax** `log buffered`  
`no log buffered`

**Default** The buffered log is configured by default.

**Mode** Global Configuration

**Examples** To configured the device to store log messages in RAM use the following commands:

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

To configure the device to not store log messages in a RAM buffer use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered
```

**Related commands**

- [clear log buffered](#)
- [copy buffered-log](#)
- [default log buffered](#)
- [log buffered \(filter\)](#)
- [log buffered size](#)
- [log buffered exclude](#)
- [show log](#)
- [show log config](#)

# log buffered (filter)

**Overview** Use this command to create a filter to select messages to be sent to the buffered log. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command removes the corresponding filter, so that the specified messages are no longer sent to the buffered log.

**Syntax** `log buffered [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`  
`no log buffered [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

| Parameter         | Description   |
|-------------------|---|
| level             | Filter messages to the buffered log by severity level.  |
| <level>           | The minimum severity of message to send to the buffered log. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:   |
| 0   emergencies   | System is unusable  |
| 1   alerts        | Action must be taken immediately  |
| 2   critical      | Critical conditions   |
| 3   errors        | Error conditions  |
| 4   warnings      | Warning conditions  |
| 5   notices       | Normal, but significant, conditions   |
| 6   informational | Informational messages  |
| 7   debugging     | Debug-level messages  |
| program           | Filter messages to the buffered log by program. Include messages from a specified program in the buffered log.  |
| <program-name>    | The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)  |
| ripng             | Routing Information Protocol - next generation (RIPng)  |
| ospf              | Open Shortest Path First (OSPF)   |
| ospfv3            | Open Shortest Path First (OSPF) version 3 (OSPFv3)  |
| bgp               | Border Gateway Protocol (BGP)   |
| rsvp              | Resource Reservation Protocol (RSVP)  |
| pim-dm            | Protocol Independent Multicast - Dense Mode (PIM-DM)  |

| Parameter                        | Description   |
|----------------------------------|---|
| <code>pim-sm</code>              | Protocol Independent Multicast - Sparse Mode (PIM-SM)   |
| <code>pim-smv6</code>            | PIM-SM version 6 (PIM-SMv6)   |
| <code>dot1x</code>               | IEEE 802.1X Port-Based Access Control   |
| <code>lacp</code>                | Link Aggregation Control Protocol (LACP)  |
| <code>stp</code>                 | Spanning Tree Protocol (STP)  |
| <code>rstp</code>                | Rapid Spanning Tree Protocol (RSTP)   |
| <code>mstp</code>                | Multiple Spanning Tree Protocol (MSTP)  |
| <code>imi</code>                 | Integrated Management Interface (IMI)   |
| <code>imish</code>               | Integrated Management Interface Shell (IMISH)   |
| <code>epsr</code>                | Ethernet Protection Switched Rings (EPSR)   |
| <code>irdp</code>                | ICMP Router Discovery Protocol (IRDP)   |
| <code>rmon</code>                | Remote Monitoring   |
| <code>loopprot</code>            | Loop Protection   |
| <code>poe</code>                 | Power-inline (Power over Ethernet)  |
| <code>dhcpsn</code>              | DHCP snooping (DHCP SN)   |
| <code>facility</code>            | Filter messages to the buffered log by syslog facility.   |
| <code>&lt;facility&gt;</code>    | Specify one of the following syslog facilities to include messages from in the buffered log:                            |
| <code>kern</code>                | Kernel messages   |
| <code>user</code>                | Random user-level messages  |
| <code>mail</code>                | Mail system   |
| <code>daemon</code>              | System daemons  |
| <code>auth</code>                | Security/authorization messages   |
| <code>syslog</code>              | Messages generated internally by syslogd  |
| <code>lpr</code>                 | Line printer subsystem  |
| <code>news</code>                | Network news subsystem  |
| <code>uucp</code>                | UUCP subsystem  |
| <code>cron</code>                | Clock daemon  |
| <code>authpriv</code>            | Security/authorization messages (private)   |
| <code>ftp</code>                 | FTP daemon  |
| <code>msgtext</code>             | Select messages containing a certain text string.   |
| <code>&lt;text-string&gt;</code> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** By default the buffered log has a filter to select messages whose severity level is “notices (5)” or higher. This filter may be removed using the **no** variant of this command.

**Mode** Global Configuration

**Examples** To add a filter to send all messages containing the text “Bridging initialization” to the buffered log, use the following commands:

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

To remove a filter that sends all messages containing the text “Bridging initialization” to the buffered log, use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered msgtext Bridging initialization
```

**Related commands**

- [clear log buffered](#)
- [default log buffered](#)
- [log buffered](#)
- [log buffered size](#)
- [log buffered exclude](#)
- [show log](#)
- [show log config](#)



# log buffered exclude

**Overview** Use this command to exclude specified log messages from the buffered log. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

**Syntax** `log buffered exclude [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`  
`no log buffered exclude [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

| Parameter         | Description  |
|-------------------|--|
| level             | Exclude messages of the specified severity level.  |
| <level>           | The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:  |
| 0   emergencies   | System is unusable   |
| 1   alerts        | Action must be taken immediately   |
| 2   critical      | Critical conditions  |
| 3   errors        | Error conditions   |
| 4   warnings      | Warning conditions   |
| 5   notices       | Normal, but significant, conditions  |
| 6   informational | Informational messages   |
| 7   debugging     | Debug-level messages   |
| program           | Exclude messages from a specified program.   |
| <program-name>    | The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)   |
| ripng             | Routing Information Protocol - next generation (RIPng)   |
| ospf              | Open Shortest Path First (OSPF)  |
| ospfv3            | Open Shortest Path First (OSPF) version 3 (OSPFv3)   |
| bgp               | Border Gateway Protocol (BGP)  |

| Parameter     | Description   |
|---------------|---|
| rsvp          | Resource Reservation Protocol (RSVP)  |
| pim-dm        | Protocol Independent Multicast - Dense Mode (PIM-DM)  |
| pim-sm        | Protocol Independent Multicast - Sparse Mode (PIM-SM)   |
| pim-smv6      | PIM-SM version 6 (PIM-SMv6)   |
| dot1x         | IEEE 802.1X Port-Based Access Control   |
| lacp          | Link Aggregation Control Protocol (LACP)  |
| stp           | Spanning Tree Protocol (STP)  |
| rstp          | Rapid Spanning Tree Protocol (RSTP)   |
| mstp          | Multiple Spanning Tree Protocol (MSTP)  |
| imi           | Integrated Management Interface (IMI)   |
| imish         | Integrated Management Interface Shell (IMISH)   |
| epsr          | Ethernet Protection Switched Rings (EPSR)   |
| irdp          | ICMP Router Discovery Protocol (IRDP)   |
| rmon          | Remote Monitoring   |
| loopprot      | Loop Protection   |
| poe           | Power-inline (Power over Ethernet)  |
| dhcpsn        | DHCP snooping (DHPCPSN)   |
| facility      | Exclude messages from a syslog facility.  |
| <facility>    | Specify one of the following syslog facilities to exclude messages from:  |
| kern          | Kernel messages   |
| user          | Random user-level messages  |
| mail          | Mail system   |
| daemon        | System daemons  |
| auth          | Security/authorization messages   |
| syslog        | Messages generated internally by syslogd  |
| lpr           | Line printer subsystem  |
| news          | Network news subsystem  |
| uucp          | UUCP subsystem  |
| cron          | Clock daemon  |
| authpriv      | Security/authorization messages (private)   |
| ftp           | FTP daemon  |
| msgtext       | Exclude messages containing a certain text string.  |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** No log messages are excluded

**Mode** Global configuration

**Example** To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered exclude msgtext example of
irrelevant message
```

**Related commands**

- clear log buffered
- default log buffered
- log buffered
- log buffered (filter)
- log buffered size
- show log
- show log config

# log buffered size

**Overview** This command configures the amount of memory that the buffered log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

Use the **no** variant of this command to return to the default.

**Syntax** log buffered size <50-250>  
no log buffered size

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

**Default** 50 kilobytes

**Mode** Global Configuration

**Example** To allow the buffered log to use up to 100 kilobytes of RAM, use the commands:

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

To return to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# no log buffered size
```

**Related commands**

- clear log buffered
- copy buffered-log
- default log buffered
- log buffered
- log buffered (filter)
- log buffered exclude
- show log
- show log config

# log console

**Overview** This command configures the device to send log messages to consoles. The console log is configured by default to send messages to the device's main console port.

Use the **no** variant of this command to configure the device not to send log messages to consoles.

**Syntax** `log console`  
`no log console`

**Mode** Global Configuration

**Examples** To configure the device to send log messages use the following commands:

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

To configure the device not to send log messages in all consoles use the following commands:

```
awplus# configure terminal
awplus(config)# no log console
```

**Related commands** [default log console](#)  
[log console \(filter\)](#)  
[log console exclude](#)  
[show log config](#)

# log console (filter)

**Overview** This command creates a filter to select messages to be sent to all consoles when the **log console** command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

**Syntax** `log console [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`  
`no log console [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

| Parameter         | Description   |
|-------------------|---|
| level             | Filter messages by severity level.  |
| <level>           | The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:   |
| 0   emergencies   | System is unusable  |
| 1   alerts        | Action must be taken immediately  |
| 2   critical      | Critical conditions   |
| 3   errors        | Error conditions  |
| 4   warnings      | Warning conditions  |
| 5   notices       | Normal, but significant, conditions   |
| 6   informational | Informational messages  |
| 7   debugging     | Debug-level messages  |
| program           | Filter messages by program. Include messages from a specified program.  |
| <program-name>    | The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)  |
| ripng             | Routing Information Protocol - next generation (RIPng)  |
| ospf              | Open Shortest Path First (OSPF)   |
| ospfv3            | Open Shortest Path First (OSPF) version 3 (OSPFv3)  |
| bgp               | Border Gateway Protocol (BGP)   |
| rsvp              | Resource Reservation Protocol (RSVP)  |
| pim-dm            | Protocol Independent Multicast - Dense Mode (PIM-DM)  |
| pim-sm            | Protocol Independent Multicast - Sparse Mode (PIM-SM)   |
| pim-smv6          | PIM-SM version 6 (PIM-SMv6)   |

| Parameter     | Description   |
|---------------|---|
| dot1x         | IEEE 802.1X Port-Based Access Control   |
| lacp          | Link Aggregation Control Protocol (LACP)  |
| stp           | Spanning Tree Protocol (STP)  |
| rstp          | Rapid Spanning Tree Protocol (RSTP)   |
| mstp          | Multiple Spanning Tree Protocol (MSTP)  |
| imi           | Integrated Management Interface (IMI)   |
| imish         | Integrated Management Interface Shell (IMISH)   |
| epsr          | Ethernet Protection Switched Rings (EPSR)   |
| irdp          | ICMP Router Discovery Protocol (IRDP)   |
| rmon          | Remote Monitoring   |
| loopprot      | Loop Protection   |
| poe           | Power-inline (Power over Ethernet)  |
| dhcpcsn       | DHCP snooping (DHPCPSN)   |
| facility      | Filter messages by syslog facility.   |
| <facility>    | Specify one of the following syslog facilities to include messages from:  |
| kern          | Kernel messages   |
| user          | Random user-level messages  |
| mail          | Mail system   |
| daemon        | System daemons  |
| auth          | Security/authorization messages   |
| syslog        | Messages generated internally by syslogd  |
| lpr           | Line printer subsystem  |
| news          | Network news subsystem  |
| uucp          | UUCP subsystem  |
| cron          | Clock daemon  |
| authpriv      | Security/authorization messages (private)   |
| ftp           | FTP daemon  |
| msgtext       | Select messages containing a certain text string.   |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** By default the console log has a filter to select messages whose severity level is **critical** or higher. This filter may be removed using the **no** variant of this command. This filter may be removed and replaced by filters that are more selective.

**Mode** Global Configuration

**Examples** To create a filter to send all messages containing the text "Bridging initialization" to console instances where the **log console** command has been entered, use the following commands:

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

To remove a default filter that includes sending **critical**, **alert** and **emergency** level messages to the console, use the following commands:

```
awplus# configure terminal
awplus(config)# no log console level critical
```

**Related commands**

- default log console
- log console
- log console exclude
- show log config



# log console exclude

**Overview** Use this command to prevent specified log messages from being sent to the console, when console logging is turned on. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

**Syntax** `log console exclude [level <level>] [program <program-name>]  
[facility <facility>] [msgtext <text-string>]`  
`no log console exclude [level <level>] [program <program-name>]  
[facility <facility>] [msgtext <text-string>]`

| Parameter         | Description  |
|-------------------|--|
| level             | Exclude messages of the specified severity level.  |
| <level>           | The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:  |
| 0   emergencies   | System is unusable   |
| 1   alerts        | Action must be taken immediately   |
| 2   critical      | Critical conditions  |
| 3   errors        | Error conditions   |
| 4   warnings      | Warning conditions   |
| 5   notices       | Normal, but significant, conditions  |
| 6   informational | Informational messages   |
| 7   debugging     | Debug-level messages   |
| program           | Exclude messages from a specified program.   |
| <program-name>    | The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)   |
| ripng             | Routing Information Protocol - next generation (RIPng)   |
| ospf              | Open Shortest Path First (OSPF)  |
| ospfv3            | Open Shortest Path First (OSPF) version 3 (OSPFv3)   |

| Parameter  | Description  |
|------------|--|
| bgp        | Border Gateway Protocol (BGP)  |
| rsvp       | Resource Reservation Protocol (RSVP)                                     |
| pim-dm     | Protocol Independent Multicast - Dense Mode (PIM-DM)                     |
| pim-sm     | Protocol Independent Multicast - Sparse Mode (PIM-SM)                    |
| pim-smv6   | PIM-SM version 6 (PIM-SMv6)  |
| dot1x      | IEEE 802.1X Port-Based Access Control                                    |
| lacp       | Link Aggregation Control Protocol (LACP)                                 |
| stp        | Spanning Tree Protocol (STP)   |
| rstp       | Rapid Spanning Tree Protocol (RSTP)                                      |
| mstp       | Multiple Spanning Tree Protocol (MSTP)                                   |
| imi        | Integrated Management Interface (IMI)                                    |
| imish      | Integrated Management Interface Shell (IMISH)                            |
| epsr       | Ethernet Protection Switched Rings (EPSR)                                |
| irdp       | ICMP Router Discovery Protocol (IRDP)                                    |
| rmon       | Remote Monitoring  |
| loopprot   | Loop Protection  |
| poe        | Power-inline (Power over Ethernet)                                       |
| dhcpsn     | DHCP snooping (DHCP SN)  |
| facility   | Exclude messages from a syslog facility.                                 |
| <facility> | Specify one of the following syslog facilities to exclude messages from: |
| kern       | Kernel messages  |
| user       | Random user-level messages   |
| mail       | Mail system  |
| daemon     | System daemons   |
| auth       | Security/authorization messages  |
| syslog     | Messages generated internally by syslogd                                 |
| lpr        | Line printer subsystem   |
| news       | Network news subsystem   |
| uucp       | UUCP subsystem   |
| cron       | Clock daemon   |
| authpriv   | Security/authorization messages (private)                                |
| ftp        | FTP daemon   |

| Parameter     | Description   |
|---------------|---|
| msgtext       | Exclude messages containing a certain text string.  |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** No log messages are excluded

**Mode** Global configuration

**Example** To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log console exclude msgtext example of
irrelevant message
```

**Related commands**

- [default log console](#)
- [log console](#)
- [log console \(filter\)](#)
- [show log config](#)

# log date-format

**Overview** Use this command to change the date format for log messages to an ISO 8601 compliant format, or to return to the default date format.

**Syntax** `log date-format {iso|default}`

| Parameter | Description   |
|-----------|---|
| iso       | Display the date and time in the ISO 8601 compliant format of: YYYY-MM-DDThh:mm:ssTZD |
| default   | Display the date and time in the default date format of YYYY MMM DD HH:MM:SS          |

**Default** The default option of YYYY MMM DD HH:MM:SS (except when using terminal monitor, when it is HH:MM:SS)

**Mode** Global Configuration

**Usage notes** In the ISO 8601 compliant format, a T separates the date from the time, and the time is followed by the timezone offset from UTC time. For example, this is a log message with an ISO 8601 compliant date:

```
2016-09-29T08:55:43+13:00 user.notice Gateway IMISH[1983]:  
[manager@ttyS0]show run
```

This is a log message with the default date format:

```
2016 Sep 29 08:55:43 user.notice Gateway IMISH[1983]:  
[manager@ttyS0]show run
```

The date format setting affects all log messages, no matter where the messages are stored or displayed.

**Examples** To set the date format to the ISO 8601 compliant format, use the commands:

```
awplus# configure terminal  
awplus(config)# log date-format iso
```

To return to the default date format of YYYY MMM DD HH:MM:SS, use the commands:

```
awplus# configure terminal  
awplus(config)# log date-format default
```

**Related commands** [show exception log](#)  
[show log](#)  
[show log permanent](#)

**Command changes** Version 5.4.6-2.1: command added

# log email

**Overview** This command configures the device to send log messages to an email address. The email address is specified in this command.

**Syntax** `log email <email-address>`

| Parameter                          | Description                               |
|------------------------------------|---|
| <code>&lt;email-address&gt;</code> | The email address to send log messages to |

**Default** By default no filters are defined for email log targets. Filters must be defined before messages will be sent.

**Mode** Global Configuration

**Example** To have log messages emailed to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com
```

**Related commands**

- [default log email](#)
- [log email \(filter\)](#)
- [log email exclude](#)
- [log email time](#)
- [show log config](#)

# log email (filter)

**Overview** This command creates a filter to select messages to be sent to an email address. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a specified email address. All configuration relating to this log target will be removed.

**Syntax** `log email <email-address> [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`  
`no log email <email-address> [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

| Parameter                          | Description   |
|------------------------------------|---|
| <code>&lt;email-address&gt;</code> | The email address to send logging messages to   |
| <code>level</code>                 | Filter messages by severity level.  |
| <code>&lt;level&gt;</code>         | The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:   |
| 0                                  | emergencies System is unusable  |
| 1                                  | alerts Action must be taken immediately   |
| 2                                  | critical Critical conditions  |
| 3                                  | errors Error conditions   |
| 4                                  | warnings Warning conditions   |
| 5                                  | notices Normal, but significant, conditions   |
| 6                                  | informational Informational messages  |
| 7                                  | debugging Debug-level messages  |
| <code>program</code>               | Filter messages by program. Include messages from a specified program.  |
| <code>&lt;program-name&gt;</code>  | The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip                                | Routing Information Protocol (RIP)  |
| ripng                              | Routing Information Protocol - next generation (RIPng)  |
| ospf                               | Open Shortest Path First (OSPF)   |
| ospfv3                             | Open Shortest Path First (OSPF) version 3 (OSPFv3)  |
| bgp                                | Border Gateway Protocol (BGP)   |

| Parameter     | Description   |
|---------------|---|
| rsvp          | Resource Reservation Protocol (RSVP)  |
| pim-dm        | Protocol Independent Multicast - Dense Mode (PIM-DM)  |
| pim-sm        | Protocol Independent Multicast - Sparse Mode (PIM-SM)   |
| pim-smv6      | PIM-SM version 6 (PIM-SMv6)   |
| dot1x         | IEEE 802.1X Port-Based Access Control   |
| lacp          | Link Aggregation Control Protocol (LACP)  |
| stp           | Spanning Tree Protocol (STP)  |
| rstp          | Rapid Spanning Tree Protocol (RSTP)   |
| mstp          | Multiple Spanning Tree Protocol (MSTP)  |
| imi           | Integrated Management Interface (IMI)   |
| imish         | Integrated Management Interface Shell (IMISH)   |
| epsr          | Ethernet Protection Switched Rings (EPSR)   |
| irdp          | ICMP Router Discovery Protocol (IRDP)   |
| rmon          | Remote Monitoring   |
| loopprot      | Loop Protection   |
| poe           | Power-inline (Power over Ethernet)  |
| dhcpcsn       | DHCP snooping (DHPCPSN)   |
| facility      | Filter messages by syslog facility.   |
| <facility>    | Specify one of the following syslog facilities to include messages from:  |
| kern          | Kernel messages   |
| user          | Random user-level messages  |
| mail          | Mail system   |
| daemon        | System daemons  |
| auth          | Security/authorization messages   |
| syslog        | Messages generated internally by syslogd  |
| lpr           | Line printer subsystem  |
| news          | Network news subsystem  |
| uucp          | UUCP subsystem  |
| cron          | Clock daemon  |
| authpriv      | Security/authorization messages (private)   |
| ftp           | FTP daemon  |
| msgtext       | Select messages containing a certain text string.   |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Mode** Global Configuration

**Examples** To create a filter to send all messages containing the text "Bridging initialization", to the email address admin@homebase.com, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@homebase.com msgtext "Bridging
initialization"
```

To create a filter to send messages with a severity level of **informational** and above to the email address admin@alliedtelesis.com, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com level
informational
```

To stop the device emailing log messages emailed to the email address admin@alliedtelesis.com, use the following commands:

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

To remove a filter that sends messages with a severity level of **informational** and above to the email address admin@alliedtelesis.com, use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@alliedtelesis.com level
informational
```

**Related commands**

- [default log email](#)
- [log email](#)
- [log email exclude](#)
- [log email time](#)
- [show log config](#)



# log email exclude

**Overview** Use this command to prevent specified log messages from being emailed, when the device is configured to send log messages to an email address. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

**Syntax** `log email exclude [level <level>] [program <program-name>]  
[facility <facility>] [msgtext <text-string>]`  
`no log email exclude [level <level>] [program <program-name>]  
[facility <facility>] [msgtext <text-string>]`

| Parameter         | Description  |
|-------------------|--|
| level             | Exclude messages of the specified severity level.  |
| <level>           | The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:  |
| 0   emergencies   | System is unusable   |
| 1   alerts        | Action must be taken immediately   |
| 2   critical      | Critical conditions  |
| 3   errors        | Error conditions   |
| 4   warnings      | Warning conditions   |
| 5   notices       | Normal, but significant, conditions  |
| 6   informational | Informational messages   |
| 7   debugging     | Debug-level messages   |
| program           | Exclude messages from a specified program.   |
| <program-name>    | The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)   |
| ripng             | Routing Information Protocol - next generation (RIPng)   |
| ospf              | Open Shortest Path First (OSPF)  |
| ospfv3            | Open Shortest Path First (OSPF) version 3 (OSPFv3)   |

| Parameter  | Description  |
|------------|--|
| bgp        | Border Gateway Protocol (BGP)  |
| rsvp       | Resource Reservation Protocol (RSVP)                                     |
| pim-dm     | Protocol Independent Multicast - Dense Mode (PIM-DM)                     |
| pim-sm     | Protocol Independent Multicast - Sparse Mode (PIM-SM)                    |
| pim-smv6   | PIM-SM version 6 (PIM-SMv6)  |
| dot1x      | IEEE 802.1X Port-Based Access Control                                    |
| lacp       | Link Aggregation Control Protocol (LACP)                                 |
| stp        | Spanning Tree Protocol (STP)   |
| rstp       | Rapid Spanning Tree Protocol (RSTP)                                      |
| mstp       | Multiple Spanning Tree Protocol (MSTP)                                   |
| imi        | Integrated Management Interface (IMI)                                    |
| imish      | Integrated Management Interface Shell (IMISH)                            |
| epsr       | Ethernet Protection Switched Rings (EPSR)                                |
| irdp       | ICMP Router Discovery Protocol (IRDP)                                    |
| rmon       | Remote Monitoring  |
| loopprot   | Loop Protection  |
| poe        | Power-inline (Power over Ethernet)                                       |
| dhcpsn     | DHCP snooping (DHCP SN)  |
| facility   | Exclude messages from a syslog facility.                                 |
| <facility> | Specify one of the following syslog facilities to exclude messages from: |
| kern       | Kernel messages  |
| user       | Random user-level messages   |
| mail       | Mail system  |
| daemon     | System daemons   |
| auth       | Security/authorization messages  |
| syslog     | Messages generated internally by syslogd                                 |
| lpr        | Line printer subsystem   |
| news       | Network news subsystem   |
| uucp       | UUCP subsystem   |
| cron       | Clock daemon   |
| authpriv   | Security/authorization messages (private)                                |
| ftp        | FTP daemon   |

| Parameter     | Description   |
|---------------|---|
| msgtext       | Exclude messages containing a certain text string.  |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** No log messages are excluded

**Mode** Global configuration

**Example** To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log email exclude msgtext example of irrelevant
message
```

**Related commands**

- default log email
- log email
- log email (filter)
- log email time
- show log config

# log email time

**Overview** This command configures the time used in messages sent to an email address. If the syslog server is in a different time zone to your device then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

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

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

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

**Mode** Global Configuration

**Usage notes** Use the **local** option if the email recipient is in the same time zone as this device. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the email recipient in hours. Messages will display the time they were generated on this device but converted to the time zone of the email recipient.

**Examples** To send messages to the email address `test@home.com` in the same time zone as the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local 0
```

To send messages to the email address `admin@base.com` with the time information converted to the time zone of the email recipient, which is 3 hours ahead of the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local-offset plus
3
```

To send messages to the email address `user@remote.com` with the time information converted to the time zone of the email recipient, which is 3 hours behind the device's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email user@remote.com time utc-offset minus
3
```

**Related commands**

- [default log email](#)
- [log email](#)
- [log email \(filter\)](#)
- [log email exclude](#)
- [show log config](#)

# log external

**Overview** Use this command to enable external logging. External logging sends syslog messages to a file on a USB storage device.

If the file does not already exist on the storage device, it (and any specified subdirectory) will be automatically created. If the file already exists, messages are appended to it.

Use the **no** variant of this command to disable external logging.

**Syntax** `log external <filename>`  
`no log external`

| Parameter                     | Description  |
|-------------------------------|--|
| <code>&lt;filename&gt;</code> | The file and optionally directory path to store the log messages in. See <a href="#">Introduction</a> on page 61 for valid syntax. |

**Default** External logging is disabled by default.

**Mode** Global Configuration

**Usage notes** We strongly recommend using ext3 or ext4 as the file system on the external storage device. These file systems have a lower risk of file corruption occurring if the switch or firewall loses power.

You should also unmount the storage device before removing it from the switch or firewall, to avoid corrupting the log file. To unmount the device, use the **unmount** command.

**Example** To save messages to a file called "messages.log" in a directory called "log" on a USB storage device, use the command:

```
awplus# configure terminal
awplus(config)# log external usb:/log/messages.log
```

**Related commands**

- [clear log external](#)
- [default log external](#)
- [log external \(filter\)](#)
- [log external exclude](#)
- [log external rotate](#)
- [log external size](#)
- [show log config](#)
- [show log external](#)
- [unmount](#)

**Command changes** Version 5.4.7-1.1: command added

# log external (filter)

**Overview** Use this command to create a filter to select messages to be sent to the external log. You can include messages based on:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

The **no** variant of this command removes the corresponding filter, so that the specified messages are no longer sent to the external log.

**Syntax** `log external [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`  
`no log external [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

| Parameter         | Description   |
|-------------------|---|
| level             | Filter messages to the external log by severity level.  |
| <level>           | The minimum severity of message to send to the external log. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:   |
| 0   emergencies   | System is unusable  |
| 1   alerts        | Action must be taken immediately  |
| 2   critical      | Critical conditions   |
| 3   errors        | Error conditions  |
| 4   warnings      | Warning conditions  |
| 5   notices       | Normal, but significant, conditions   |
| 6   informational | Informational messages  |
| 7   debugging     | Debug-level messages  |
| program           | Filter messages to the external log by program. Include messages from a specified program in the external log.  |
| <program-name>    | The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)  |
| ripng             | Routing Information Protocol - next generation (RIPng)  |
| ospf              | Open Shortest Path First (OSPF)   |



| Parameter  | Description   |
|------------|---|
| ospfv3     | Open Shortest Path First (OSPF) version 3 (OSPFv3)                                  |
| bgp        | Border Gateway Protocol (BGP)   |
| rsvp       | Resource Reservation Protocol (RSVP)  |
| pim-dm     | Protocol Independent Multicast - Dense Mode (PIM-DM)                                |
| pim-sm     | Protocol Independent Multicast - Sparse Mode (PIM-SM)                               |
| pim-smv6   | PIM-SM version 6 (PIM-SMv6)   |
| dot1x      | IEEE 802.1X Port-Based Access Control   |
| lacp       | Link Aggregation Control Protocol (LACP)  |
| stp        | Spanning Tree Protocol (STP)  |
| rstp       | Rapid Spanning Tree Protocol (RSTP)   |
| mstp       | Multiple Spanning Tree Protocol (MSTP)  |
| imi        | Integrated Management Interface (IMI)   |
| imish      | Integrated Management Interface Shell (IMISH)                                       |
| epsr       | Ethernet Protection Switched Rings (EPSR)   |
| irdp       | ICMP Router Discovery Protocol (IRDP)   |
| rmon       | Remote Monitoring   |
| loopprot   | Loop Protection   |
| poe        | Power-inline (Power over Ethernet)  |
| dhcpcsn    | DHCP snooping (DHPCSN)  |
| facility   | Filter messages to the external log by syslog facility.                             |
| <facility> | Specify one of the following syslog facilities to include messages from in the log: |
| kern       | Kernel messages   |
| user       | Random user-level messages  |
| mail       | Mail system   |
| daemon     | System daemons  |
| auth       | Security/authorization messages   |
| syslog     | Messages generated internally by syslogd  |
| lpr        | Line printer subsystem  |
| news       | Network news subsystem  |
| uucp       | UUCP subsystem  |
| cron       | Clock daemon  |
| authpriv   | Security/authorization messages (private)   |
| ftp        | FTP daemon  |

| Parameter     | Description   |
|---------------|---|
| msgtext       | Select messages containing a certain text string.   |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** By default the external log has a filter to select messages whose severity level is “notices (5)” or higher. This filter may be removed using the **no** variant of this command.

**Mode** Global Configuration

**Examples** To add a filter to send all messages containing the text “Bridging initialization” to the external log, use the following commands:

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

To remove a filter that sends all messages containing the text “Bridging initialization” to the external log, use the following commands:

```
awplus# configure terminal
awplus(config)# no log external msgtext Bridging initialization
```

**Related commands**

- clear log external
- default log external
- log external
- log external exclude
- log external rotate
- log external size
- show log config
- show log external
- unmount

**Command changes** Version 5.4.7-1.1: command added

# log external exclude

**Overview** Use this command to exclude specified log messages from the external log. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

**Syntax** `log external exclude [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`  
`no log external exclude [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

| Parameter         | Description  |
|-------------------|--|
| level             | Exclude messages of the specified severity level.  |
| <level>           | The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:  |
| 0   emergencies   | System is unusable   |
| 1   alerts        | Action must be taken immediately   |
| 2   critical      | Critical conditions  |
| 3   errors        | Error conditions   |
| 4   warnings      | Warning conditions   |
| 5   notices       | Normal, but significant, conditions  |
| 6   informational | Informational messages   |
| 7   debugging     | Debug-level messages   |
| program           | Exclude messages from a specified program.   |
| <program-name>    | The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)   |
| ripng             | Routing Information Protocol - next generation (RIPng)   |
| ospf              | Open Shortest Path First (OSPF)  |
| ospfv3            | Open Shortest Path First (OSPF) version 3 (OSPFv3)   |
| bgp               | Border Gateway Protocol (BGP)  |

| Parameter     | Description   |
|---------------|---|
| rsvp          | Resource Reservation Protocol (RSVP)  |
| pim-dm        | Protocol Independent Multicast - Dense Mode (PIM-DM)  |
| pim-sm        | Protocol Independent Multicast - Sparse Mode (PIM-SM)   |
| pim-smv6      | PIM-SM version 6 (PIM-SMv6)   |
| dot1x         | IEEE 802.1X Port-Based Access Control   |
| lacp          | Link Aggregation Control Protocol (LACP)  |
| stp           | Spanning Tree Protocol (STP)  |
| rstp          | Rapid Spanning Tree Protocol (RSTP)   |
| mstp          | Multiple Spanning Tree Protocol (MSTP)  |
| imi           | Integrated Management Interface (IMI)   |
| imish         | Integrated Management Interface Shell (IMISH)   |
| epsr          | Ethernet Protection Switched Rings (EPSR)   |
| irdp          | ICMP Router Discovery Protocol (IRDP)   |
| rmon          | Remote Monitoring   |
| loopprot      | Loop Protection   |
| poe           | Power-inline (Power over Ethernet)  |
| dhcpsn        | DHCP snooping (DHCP SN)   |
| facility      | Exclude messages from a syslog facility.  |
| <facility>    | Specify one of the following syslog facilities to exclude messages from:  |
| kern          | Kernel messages   |
| user          | Random user-level messages  |
| mail          | Mail system   |
| daemon        | System daemons  |
| auth          | Security/authorization messages   |
| syslog        | Messages generated internally by syslogd  |
| lpr           | Line printer subsystem  |
| news          | Network news subsystem  |
| uucp          | UUCP subsystem  |
| cron          | Clock daemon  |
| authpriv      | Security/authorization messages (private)   |
| ftp           | FTP daemon  |
| msgtext       | Exclude messages containing a certain text string.  |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** No log messages are excluded

**Mode** Global Configuration

**Example** To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log external exclude msgtext example of
irrelevant message
```

**Related  
commands** [clear log external](#)  
[default log external](#)

[log external](#)

[log external \(filter\)](#)

[log external rotate](#)

[log external size](#)

[show log config](#)

[show log external](#)

[unmount](#)

**Command  
changes** Version 5.4.7-1.1: command added

# log external rotate

**Overview** Use this command to configure the number of files that the external log can rotate through.

Use the **no** variant of this command to return to the default.

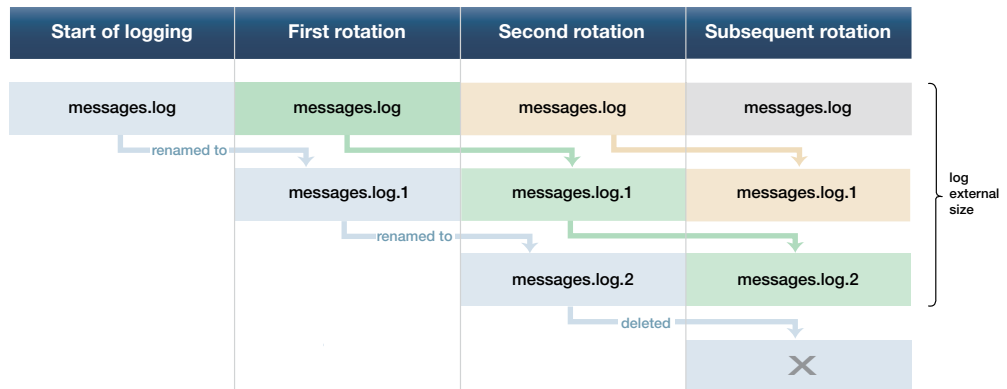
**Syntax** `log external rotate <0-255>`  
`no log external rotate`

| Parameter                  | Description   |
|----------------------------|---|
| <code>&lt;0-255&gt;</code> | The number of additional files to rotate through. Note that the device rotates between the initial file and the number of additional files specified by this value - see the Usage section below. |

**Default** The default is 1, which rotates between the initial file and 1 additional file (for example, rotates between `messages.log` and `messages.log.1`)

**Mode** Global Configuration

**Usage notes** The device rotates between the initial file and the number of additional files specified by this command. For example, the diagram below shows how setting rotate to 2 makes the device rotate through 3 files.



Note that if you set rotate to 0, and the external log file becomes full, then the device deletes the full log file and creates a new (empty) file of the same name to save messages into. For this reason, we recommend setting rotate to at least 1.

**Example** To set the rotation value to 2, and therefore rotate between 3 files, use the commands:

```
awplus# configure terminal
awplus(config)# log external rotate 2
```

**Related commands** [clear log external](#)

default log external  
log external  
log external (filter)  
log external exclude  
log external size  
show log config  
show log external  
unmount

**Command changes** Version 5.4.7-1.1: command added

# log external size

**Overview** Use this command to configure the total amount of size that the external log is permitted to use, in kilobytes. The maximum possible depends on the storage device's file system.

Note that if you are rotating between multiple files, this is the maximum size of all files, not of each individual file. For example, if you are rotating between 2 files (**log external rotate 1**), each file will have a maximum size of 25 kBytes by default.

Use the **no** variant of this command to return to the default size.

**Syntax** `log external size [<50-4194304>]`  
`no log external size`

| Parameter    | Description   |
|--------------|---|
| <50-4194304> | The total amount of size that the external log is permitted to use, in kilobytes. |

**Default** 50 kBytes

**Mode** Global Configuration

**Example** To configure a total log size of 100 kBytes, use the commands:

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

**Related commands**

- [clear log external](#)
- [default log external](#)
- [log external](#)
- [log external \(filter\)](#)
- [log external exclude](#)
- [log external rotate](#)
- [log external size](#)
- [show log config](#)
- [show log external](#)
- [unmount](#)

**Command changes** Version 5.4.7-1.1: command added



# log facility

**Overview** Use this command to assign a facility to all log messages generated on this device. This facility overrides any facility that is automatically generated as part of the log message.

Use the **no** variant of this command to remove the configured facility.

**Syntax** `log facility {kern|user|mail|daemon|auth|syslog|lpr|news|uucp|cron|authpriv|ftp|local0|local1|local2|local3|local4|local5|local6|local7}`

`no log facility`

**Default** None. The outgoing syslog facility depends on the log message.

**Mode** Global Configuration

**Usage notes** Specifying different facilities for log messages generated on different devices can allow messages from multiple devices sent to a common server to be distinguished from each other.

Ordinarily, the facility values generated in log messages have meanings as shown in the following table. Using this command will override these meanings, and the new meanings will depend on the use you put them to.

Table 7-1: Ordinary meanings of the facility parameter in log messages

| Facility | Description  |
|----------|--|
| kern     | Kernel messages                                    |
| user     | User-level messages                                |
| mail     | Mail system  |
| daemon   | System daemons                                     |
| auth     | Security/authorization messages                    |
| syslog   | Messages generated internally by the syslog daemon |
| lpr      | Line printer subsystem                             |
| news     | Network news subsystem                             |
| uucp     | UNIX-to-UNIX Copy Program subsystem                |
| cron     | Clock daemon                                       |
| authpriv | Security/authorization (private) messages          |

Table 7-1: Ordinary meanings of the facility parameter in log messages (cont.)

| Facility    | Description   |
|-------------|---|
| ftp         | FTP daemon  |
| local<0..7> | The facility labels above have specific meanings, while the local facility labels are intended to be put to local use. In AlliedWare Plus, some of these local facility labels are used in log messages. In particular, local5 is assigned to log messages generated by UTM Firewall security features. |

**Example** To specify a facility of local6, use the following commands:

```
awplus# configure terminal  
awplus(config)# log facility local6
```

**Related commands** [show log config](#)

# log host

**Overview** This command configures the device to send log messages to a remote syslog server via UDP port 514. The IP address of the remote server must be specified. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent.

Use the **no** variant of this command to stop sending log messages to the remote syslog server.

**Syntax**

```
log host <ipv4-addr> [secure]
log host <ipv6-addr>
no log host <ipv4-addr>|<ipv6-addr>
```

| Parameter   | Description  |
|-------------|--|
| <ipv4-addr> | Specify the source IPv4 address, in dotted decimal notation (A.B.C.D).                       |
| <ipv6-addr> | Specify the source IPv6 address, in X::X::X::X notation.                                     |
| secure      | Optional value to create a secure log destination. This option is only valid for IPv4 hosts. |

**Mode** Global Configuration

**Usage notes** Use the optional **secure** parameter to configure a secure IPv4 syslog host. For secure hosts, syslog over TLS is used to encrypt the logs. The certificate received from the remote log server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

The remote server may also request that a certificate is transmitted from the local device. In this situation the first trustpoint added to the syslog application will be transmitted to the remote server.

For detailed information about securing syslog, see the [PKI Feature Overview\\_and Configuration\\_Guide](#).

**Examples** To configure the device to send log messages to a remote secure syslog server with IP address 10.32.16.99, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.99 secure
```

To stop the device from sending log messages to the remote syslog server with IP address 10.32.16.99, use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.99
```

**Related commands**

- [default log host](#)
- [log host \(filter\)](#)

log host exclude  
log host source  
log host startup-delay  
log host time  
log trustpoint  
show log config

# log host (filter)

**Overview** This command creates a filter to select messages to be sent to a remote syslog server. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a substring within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a remote syslog server. The IP address of the syslog server must be specified. All configuration relating to this log target will be removed.

**Syntax** `log host <ip-addr> [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`  
`no log host <ip-addr> [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

| Parameter                         | Description   |
|-----------------------------------|---|
| <code>&lt;ip-addr&gt;</code>      | The IP address of a remote syslog server.   |
| <code>level</code>                | Filter messages by severity level.  |
| <code>&lt;level&gt;</code>        | The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:   |
| 0   emergencies                   | System is unusable  |
| 1   alerts                        | Action must be taken immediately  |
| 2   critical                      | Critical conditions   |
| 3   errors                        | Error conditions  |
| 4   warnings                      | Warning conditions  |
| 5   notices                       | Normal, but significant, conditions   |
| 6   informational                 | Informational messages  |
| 7   debugging                     | Debug-level messages  |
| <code>program</code>              | Filter messages by program. Include messages from a specified program.  |
| <code>&lt;program-name&gt;</code> | The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip                               | Routing Information Protocol (RIP)  |
| ripng                             | Routing Information Protocol - next generation (RIPng)  |
| ospf                              | Open Shortest Path First (OSPF)   |
| ospfv3                            | Open Shortest Path First (OSPF) version 3 (OSPFv3)  |
| bgp                               | Border Gateway Protocol (BGP)   |
| rsvp                              | Resource Reservation Protocol (RSVP)  |

| Parameter     | Description   |
|---------------|---|
| pim-dm        | Protocol Independent Multicast - Dense Mode (PIM-DM)  |
| pim-sm        | Protocol Independent Multicast - Sparse Mode (PIM-SM)   |
| pim-smv6      | PIM-SM version 6 (PIM-SMv6)   |
| dot1x         | IEEE 802.1X Port-Based Access Control   |
| lacp          | Link Aggregation Control Protocol (LACP)  |
| stp           | Spanning Tree Protocol (STP)  |
| rstp          | Rapid Spanning Tree Protocol (RSTP)   |
| mstp          | Multiple Spanning Tree Protocol (MSTP)  |
| imi           | Integrated Management Interface (IMI)   |
| imish         | Integrated Management Interface Shell (IMISH)   |
| epsr          | Ethernet Protection Switched Rings (EPSR)   |
| irdp          | ICMP Router Discovery Protocol (IRDP)   |
| rmon          | Remote Monitoring   |
| loopprot      | Loop Protection   |
| poe           | Power-inline (Power over Ethernet)  |
| dhcpcsn       | DHCP snooping (DHPCPSN)   |
| facility      | Filter messages by syslog facility.   |
| <facility>    | Specify one of the following syslog facilities to include messages from:  |
| kern          | Kernel messages   |
| user          | Random user-level messages  |
| mail          | Mail system   |
| daemon        | System daemons  |
| auth          | Security/authorization messages   |
| syslog        | Messages generated internally by syslogd  |
| lpr           | Line printer subsystem  |
| news          | Network news subsystem  |
| uucp          | UUCP subsystem  |
| cron          | Clock daemon  |
| authpriv      | Security/authorization messages (private)   |
| ftp           | FTP daemon  |
| msgtext       | Select messages containing a certain text string.   |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Mode** Global Configuration

**Examples** To create a filter to send all messages containing the text "Bridging initialization", to a remote syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 msgtext "Bridging
initialization"
```

To create a filter to send messages with a severity level of **informational** and above to the syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 level informational
```

To remove a filter that sends all messages containing the text "Bridging initialization", to a remote syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.21 msgtext "Bridging
initialization"
```

To remove a filter that sends messages with a severity level of **informational** and above to the syslog server with IP address 10.32.16.21, use the following commands:

```
awplusawpluls# configure terminal
awplus(config)# no log host 10.32.16.21 level informational
```

**Related commands**

- default log host
- log host
- log host exclude
- log host source
- log host time
- show log config

# log host exclude

**Overview** Use this command to prevent specified log messages from being sent to the remote syslog server, when `log host` is enabled. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

**Syntax** `log host exclude [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`  
`no log host exclude [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

| Parameter         | Description  |
|-------------------|--|
| level             | Exclude messages of the specified severity level.  |
| <level>           | The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:  |
| 0   emergencies   | System is unusable   |
| 1   alerts        | Action must be taken immediately   |
| 2   critical      | Critical conditions  |
| 3   errors        | Error conditions   |
| 4   warnings      | Warning conditions   |
| 5   notices       | Normal, but significant, conditions  |
| 6   informational | Informational messages   |
| 7   debugging     | Debug-level messages   |
| program           | Exclude messages from a specified program.   |
| <program-name>    | The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)   |
| ripng             | Routing Information Protocol - next generation (RIPng)   |
| ospf              | Open Shortest Path First (OSPF)  |
| ospfv3            | Open Shortest Path First (OSPF) version 3 (OSPFv3)   |



| Parameter  | Description  |
|------------|--|
| bgp        | Border Gateway Protocol (BGP)  |
| rsvp       | Resource Reservation Protocol (RSVP)                                     |
| pim-dm     | Protocol Independent Multicast - Dense Mode (PIM-DM)                     |
| pim-sm     | Protocol Independent Multicast - Sparse Mode (PIM-SM)                    |
| pim-smv6   | PIM-SM version 6 (PIM-SMv6)  |
| dot1x      | IEEE 802.1X Port-Based Access Control                                    |
| lacp       | Link Aggregation Control Protocol (LACP)                                 |
| stp        | Spanning Tree Protocol (STP)   |
| rstp       | Rapid Spanning Tree Protocol (RSTP)                                      |
| mstp       | Multiple Spanning Tree Protocol (MSTP)                                   |
| imi        | Integrated Management Interface (IMI)                                    |
| imish      | Integrated Management Interface Shell (IMISH)                            |
| epsr       | Ethernet Protection Switched Rings (EPSR)                                |
| irdp       | ICMP Router Discovery Protocol (IRDP)                                    |
| rmon       | Remote Monitoring  |
| loopprot   | Loop Protection  |
| poe        | Power-inline (Power over Ethernet)                                       |
| dhcpsn     | DHCP snooping (DHCP SN)  |
| facility   | Exclude messages from a syslog facility.                                 |
| <facility> | Specify one of the following syslog facilities to exclude messages from: |
| kern       | Kernel messages  |
| user       | Random user-level messages   |
| mail       | Mail system  |
| daemon     | System daemons   |
| auth       | Security/authorization messages  |
| syslog     | Messages generated internally by syslogd                                 |
| lpr        | Line printer subsystem   |
| news       | Network news subsystem   |
| uucp       | UUCP subsystem   |
| cron       | Clock daemon   |
| authpriv   | Security/authorization messages (private)                                |
| ftp        | FTP daemon   |

| Parameter     | Description   |
|---------------|---|
| msgtext       | Exclude messages containing a certain text string.  |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** No log messages are excluded

**Mode** Global configuration

**Example** To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log host exclude msgtext example of irrelevant
message
```

**Related commands**

- default log host
- log host
- log host (filter)
- log host source
- log host time
- show log config

# log host source

**Overview** Use this command to specify a source interface or IP address for the device to send syslog messages from. You can specify any one of an interface name, an IPv4 address or an IPv6 address.

This is useful if the device can reach the syslog server via multiple interfaces or addresses and you want to control which interface/address the device uses.

Note that AlliedWare Plus does not support source interface settings on secure log hosts (which are hosts configured using "log host <ip-address> secure").

Use the **no** variant of this command to stop specifying a source interface or address.

**Syntax** `log host source {<interface-name>|<ipv4-addr>|<ipv6-addr>}`  
`no log host source`

| Parameter        | Description   |
|------------------|---|
| <interface-name> | Specify the source interface name. You can enter a VLAN, eth interface or loopback interface. |
| <ipv4-addr>      | Specify the source IPv4 address, in dotted decimal notation (A.B.C.D).                        |
| <ipv6-addr>      | Specify the source IPv6 address, in X:X::X:X notation.  |

**Default** None (no source is configured)

**Mode** Global Configuration

**Example** To send syslog messages from 192.168.1.1, use the commands:

```
awplus# configure terminal
awplus(config)# log host source 192.168.1.1
```

**Related commands**

- [default log host](#)
- [log host](#)
- [log host \(filter\)](#)
- [log host exclude](#)
- [log host time](#)
- [show log config](#)

# log host startup-delay

**Overview** Use this command to set the delay between the device booting up and it attempting to connect to remote log hosts. This is to allow time for network connectivity to the remote host to be established. During this period, the device buffers log messages and sends them once it has connected to the remote host.

The startup delay begins when the message "syslog-ng starting up" appears in the log.

If the default startup delay is not long enough for the boot and configuration process to complete and the links to come up, you may see logging failure messages on startup. In these cases, you can use the command to increase the startup delay.

Use the **no** variant of this command to return to the default delay values.

**Syntax** `log host startup-delay [delay <1-600>] [messages <1-5000>]`  
`no log host startup-delay`

| Parameter                            | Description  |
|--------------------------------------|--|
| <code>delay &lt;1-600&gt;</code>     | The time, in seconds, from when syslog starts before the device attempts to filter and transmit the buffered messages to remote hosts. |
| <code>messages &lt;1-5000&gt;</code> | The maximum number of messages that the device will buffer during the delay period.  |

**Default** By default the system will buffer up to 2000 messages and wait 120 seconds from when syslog starts before attempting to filter and transmit the buffered messages to remote hosts.

**Mode** Global Configuration

**Example** To increase the delay to 180 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# log host startup-delay delay 180
```

**Related commands**

- [default log host](#)
- [log host \(filter\)](#)
- [log host exclude](#)
- [log host source](#)
- [log host time](#)
- [log trustpoint](#)
- [show log config](#)

**Command changes** Version 5.4.8-0.2: defaults changed

# log host time

**Overview** This command configures the time used in messages sent to a remote syslog server. If the syslog server is in a different time zone to your device then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

**Syntax** `log host <email-address> time {local|local-offset|utc-offset {plus|minus} <0-24>}`

| Parameter       | Description  |
|-----------------|--|
| <email-address> | The email address to send log messages to  |
| time            | Specify the time difference between the email recipient and the device you are configuring.  |
| local           | The device is in the same time zone as the email recipient   |
| local-offset    | The device is in a different time zone to the email recipient. Use the <b>plus</b> or <b>minus</b> keywords and specify the difference (offset) from local time of the device to the email recipient in hours. |
| utc-offset      | The device is in a different time zone to the email recipient. Use the <b>plus</b> or <b>minus</b> keywords and specify the difference (offset) from UTC time of the device to the email recipient in hours.   |
| plus            | Negative offset (difference) from the device to the syslog server.   |
| minus           | Positive offset (difference) from the device to the syslog server.   |
| <0-24>          | World Time zone offset in hours  |

**Default** The default is **local** time.

**Mode** Global Configuration

**Usage notes** Use the **local** option if the remote syslog server is in the same time zone as the device. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the remote syslog server in hours. Messages will display the time they were generated on this device but converted to the time zone of the remote syslog server.

**Examples** To send messages to the remote syslog server with the IP address 10.32.16.21 in the same time zone as the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 time local 0
```

To send messages to the remote syslog server with the IP address 10.32.16.12 with the time information converted to the time zone of the remote syslog server, which is 3 hours ahead of the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.12 time local-offset plus 3
```

To send messages to the remote syslog server with the IP address 10.32.16.02 with the time information converted to the time zone of the email recipient, which is 3 hours behind the device's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.02 time utc-offset minus 3
```

**Related  
commands**

[default log host](#)

[log host](#)

[log host \(filter\)](#)

[log host exclude](#)

[log host source](#)

[show log config](#)

# log monitor (filter)

**Overview** This command creates a filter to select messages to be sent to the terminal when the **terminal monitor** command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

**Syntax** `log monitor [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`  
`no log monitor [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

| Parameter         | Description   |
|-------------------|---|
| level             | Filter messages by severity level.  |
| <level>           | The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:   |
| 0   emergencies   | System is unusable  |
| 1   alerts        | Action must be taken immediately  |
| 2   critical      | Critical conditions   |
| 3   errors        | Error conditions  |
| 4   warnings      | Warning conditions  |
| 5   notices       | Normal, but significant, conditions   |
| 6   informational | Informational messages  |
| 7   debugging     | Debug-level messages  |
| program           | Filter messages by program. Include messages from a specified program.  |
| <program-name>    | The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)  |
| ripng             | Routing Information Protocol - next generation (RIPng)  |
| ospf              | Open Shortest Path First (OSPF)   |
| ospfv3            | Open Shortest Path First (OSPF) version 3 (OSPFv3)  |
| bgp               | Border Gateway Protocol (BGP)   |
| rsvp              | Resource Reservation Protocol (RSVP)  |
| pim-dm            | Protocol Independent Multicast - Dense Mode (PIM-DM)  |
| pim-sm            | Protocol Independent Multicast - Sparse Mode (PIM-SM)   |
| pim-smv6          | PIM-SM version 6 (PIM-SMv6)   |



| Parameter     | Description   |
|---------------|---|
| dot1x         | IEEE 802.1X Port-Based Access Control   |
| lacp          | Link Aggregation Control Protocol (LACP)  |
| stp           | Spanning Tree Protocol (STP)  |
| rstp          | Rapid Spanning Tree Protocol (RSTP)   |
| mstp          | Multiple Spanning Tree Protocol (MSTP)  |
| imi           | Integrated Management Interface (IMI)   |
| imish         | Integrated Management Interface Shell (IMISH)   |
| epsr          | Ethernet Protection Switched Rings (EPSR)   |
| irdp          | ICMP Router Discovery Protocol (IRDP)   |
| rmon          | Remote Monitoring   |
| loopprot      | Loop Protection   |
| poe           | Power-inline (Power over Ethernet)  |
| dhcpcsn       | DHCP snooping (DHCPSN)  |
| facility      | Filter messages by syslog facility.   |
| <facility>    | Specify one of the following syslog facilities to include messages from:  |
| kern          | Kernel messages   |
| user          | Random user-level messages  |
| mail          | Mail system   |
| daemon        | System daemons  |
| auth          | Security/authorization messages   |
| syslog        | Messages generated internally by syslogd  |
| lpr           | Line printer subsystem  |
| news          | Network news subsystem  |
| uucp          | UUCP subsystem  |
| cron          | Clock daemon  |
| authpriv      | Security/authorization messages (private)   |
| ftp           | FTP daemon  |
| msgtext       | Select messages containing a certain text string.   |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** By default there is a filter to select all messages. This filter may be removed and replaced by filters that are more selective.

**Mode** Global Configuration

**Examples** To create a filter to send all messages that are generated by authentication and have a severity of **info** or higher to terminal instances where the terminal monitor command has been given, use the following commands:

```
awplus# configure terminal
awplus(config)# log monitor level info program auth
```

To remove a default filter that includes sending everything to the terminal, use the following commands:

```
awplus# configure terminal
awplus(config)# no log monitor level debugging
```

**Related commands**

- [default log monitor](#)
- [log monitor exclude](#)
- [show log config](#)
- [terminal monitor](#)

# log monitor exclude

**Overview** Use this command to prevent specified log messages from being displayed on a terminal, when **terminal monitor** is enabled. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

**Syntax** `log console exclude [level <level>] [program <program-name>]  
[facility <facility>] [msgtext <text-string>]`  
`no log console exclude [level <level>] [program <program-name>]  
[facility <facility>] [msgtext <text-string>]`

| Parameter         | Description  |
|-------------------|--|
| level             | Exclude messages of the specified severity level.  |
| <level>           | The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:  |
| 0   emergencies   | System is unusable   |
| 1   alerts        | Action must be taken immediately   |
| 2   critical      | Critical conditions  |
| 3   errors        | Error conditions   |
| 4   warnings      | Warning conditions   |
| 5   notices       | Normal, but significant, conditions  |
| 6   informational | Informational messages   |
| 7   debugging     | Debug-level messages   |
| program           | Exclude messages from a specified program.   |
| <program-name>    | The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)   |
| ripng             | Routing Information Protocol - next generation (RIPng)   |
| ospf              | Open Shortest Path First (OSPF)  |
| ospfv3            | Open Shortest Path First (OSPF) version 3 (OSPFv3)   |

| Parameter  | Description  |
|------------|--|
| bgp        | Border Gateway Protocol (BGP)  |
| rsvp       | Resource Reservation Protocol (RSVP)                                     |
| pim-dm     | Protocol Independent Multicast - Dense Mode (PIM-DM)                     |
| pim-sm     | Protocol Independent Multicast - Sparse Mode (PIM-SM)                    |
| pim-smv6   | PIM-SM version 6 (PIM-SMv6)  |
| dot1x      | IEEE 802.1X Port-Based Access Control                                    |
| lacp       | Link Aggregation Control Protocol (LACP)                                 |
| stp        | Spanning Tree Protocol (STP)   |
| rstp       | Rapid Spanning Tree Protocol (RSTP)                                      |
| mstp       | Multiple Spanning Tree Protocol (MSTP)                                   |
| imi        | Integrated Management Interface (IMI)                                    |
| imish      | Integrated Management Interface Shell (IMISH)                            |
| epsr       | Ethernet Protection Switched Rings (EPSR)                                |
| irdp       | ICMP Router Discovery Protocol (IRDP)                                    |
| rmon       | Remote Monitoring  |
| loopprot   | Loop Protection  |
| poe        | Power-inline (Power over Ethernet)                                       |
| dhcpsn     | DHCP snooping (DHCP SN)  |
| facility   | Exclude messages from a syslog facility.                                 |
| <facility> | Specify one of the following syslog facilities to exclude messages from: |
| kern       | Kernel messages  |
| user       | Random user-level messages   |
| mail       | Mail system  |
| daemon     | System daemons   |
| auth       | Security/authorization messages  |
| syslog     | Messages generated internally by syslogd                                 |
| lpr        | Line printer subsystem   |
| news       | Network news subsystem   |
| uucp       | UUCP subsystem   |
| cron       | Clock daemon   |
| authpriv   | Security/authorization messages (private)                                |
| ftp        | FTP daemon   |

| Parameter     | Description   |
|---------------|---|
| msgtext       | Exclude messages containing a certain text string.  |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** No log messages are excluded

**Mode** Global configuration

**Example** To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log monitor exclude msgtext example of
irrelevant message
```

**Related commands**

- default log monitor
- log monitor (filter)
- show log config
- terminal monitor

# log permanent

**Overview** This command configures the device to send permanent log messages to non-volatile storage (NVS) on the device. The content of the permanent log is retained over a reboot. Once the permanent log reaches its configured maximum allowable size old messages will be deleted to make way for new messages.

The **no** variant of this command configures the device not to send any messages to the permanent log. Log messages will not be retained over a restart.

**Syntax** `log permanent`  
`no log permanent`

**Mode** Global Configuration

**Examples** To enable permanent logging use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent
```

To disable permanent logging use the following commands:

```
awplus# configure terminal
awplus(config)# no log permanent
```

**Related commands**

- `clear log permanent`
- `copy permanent-log`
- `default log permanent`
- `log permanent (filter)`
- `log permanent exclude`
- `log permanent size`
- `show log config`
- `show log permanent`

# log permanent (filter)

**Overview** This command creates a filter to select messages to be sent to the permanent log. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command removes the corresponding filter, so that the specified messages are no longer sent to the permanent log.

**Syntax** `log permanent [level <level>] [program <program-name>]  
[facility <facility>] [msgtext <text-string>]`  
`no log permanent [level <level>] [program <program-name>]  
[facility <facility>] [msgtext <text-string>]`

| Parameter         | Description   |
|-------------------|---|
| level             | Filter messages sent to the permanent log by severity level.  |
| <level>           | The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:   |
| 0   emergencies   | System is unusable  |
| 1   alerts        | Action must be taken immediately  |
| 2   critical      | Critical conditions   |
| 3   errors        | Error conditions  |
| 4   warnings      | Warning conditions  |
| 5   notices       | Normal, but significant, conditions   |
| 6   informational | Informational messages  |
| 7   debugging     | Debug-level messages  |
| program           | Filter messages by program. Include messages from a specified program.  |
| <program-name>    | The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)  |
| ripng             | Routing Information Protocol - next generation (RIPng)  |
| ospf              | Open Shortest Path First (OSPF)   |
| ospfv3            | Open Shortest Path First (OSPF) version 3 (OSPFv3)  |
| bgp               | Border Gateway Protocol (BGP)   |
| rsvp              | Resource Reservation Protocol (RSVP)  |
| pim-dm            | Protocol Independent Multicast - Dense Mode (PIM-DM)  |
| pim-sm            | Protocol Independent Multicast - Sparse Mode (PIM-SM)   |

| Parameter                        | Description   |
|----------------------------------|---|
| <code>pim-smv6</code>            | PIM-SM version 6 (PIM-SMv6)   |
| <code>dot1x</code>               | IEEE 802.1X Port-Based Access Control   |
| <code>lacp</code>                | Link Aggregation Control Protocol (LACP)  |
| <code>stp</code>                 | Spanning Tree Protocol (STP)  |
| <code>rstp</code>                | Rapid Spanning Tree Protocol (RSTP)   |
| <code>mstp</code>                | Multiple Spanning Tree Protocol (MSTP)  |
| <code>imi</code>                 | Integrated Management Interface (IMI)   |
| <code>imish</code>               | Integrated Management Interface Shell (IMISH)   |
| <code>epsr</code>                | Ethernet Protection Switched Rings (EPSR)   |
| <code>irdp</code>                | ICMP Router Discovery Protocol (IRDP)   |
| <code>rmon</code>                | Remote Monitoring   |
| <code>loopprot</code>            | Loop Protection   |
| <code>poe</code>                 | Power-inline (Power over Ethernet)  |
| <code>dhcpsn</code>              | DHCP snooping (DHCP SN)   |
| <code>facility</code>            | Filter messages by syslog facility.   |
| <code>&lt;facility&gt;</code>    | Specify one of the following syslog facilities to include messages from:  |
| <code>kern</code>                | Kernel messages   |
| <code>user</code>                | Random user-level messages  |
| <code>mail</code>                | Mail system   |
| <code>daemon</code>              | System daemons  |
| <code>auth</code>                | Security/authorization messages   |
| <code>syslog</code>              | Messages generated internally by syslogd  |
| <code>lpr</code>                 | Line printer subsystem  |
| <code>news</code>                | Network news subsystem  |
| <code>uucp</code>                | UUCP subsystem  |
| <code>cron</code>                | Clock daemon  |
| <code>authpriv</code>            | Security/authorization messages (private)   |
| <code>ftp</code>                 | FTP daemon  |
| <code>msgtext</code>             | Select messages containing a certain text string.   |
| <code>&lt;text-string&gt;</code> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** By default the buffered log has a filter to select messages whose severity level is `notices` (5) or higher. This filter may be removed using the **no** variant of this command.



**Mode** Global Configuration

**Examples** To create a filter to send all messages containing the text "Bridging initialization", to the permanent log use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# log permanent msgtext Bridging initialization
```

**Related commands**

- clear log permanent
- default log permanent
- log permanent
- log permanent exclude
- log permanent size
- show log config
- show log permanent

# log permanent exclude

**Overview** Use this command to prevent specified log messages from being sent to the permanent log. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

**Syntax** `log permanent exclude [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`  
`no log permanent exclude [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

| Parameter         | Description  |
|-------------------|--|
| level             | Exclude messages of the specified severity level.  |
| <level>           | The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:  |
| 0   emergencies   | System is unusable   |
| 1   alerts        | Action must be taken immediately   |
| 2   critical      | Critical conditions  |
| 3   errors        | Error conditions   |
| 4   warnings      | Warning conditions   |
| 5   notices       | Normal, but significant, conditions  |
| 6   informational | Informational messages   |
| 7   debugging     | Debug-level messages   |
| program           | Exclude messages from a specified program.   |
| <program-name>    | The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. |
| rip               | Routing Information Protocol (RIP)   |
| ripng             | Routing Information Protocol - next generation (RIPng)   |
| ospf              | Open Shortest Path First (OSPF)  |
| ospfv3            | Open Shortest Path First (OSPF) version 3 (OSPFv3)   |
| bgp               | Border Gateway Protocol (BGP)  |

| Parameter     | Description   |
|---------------|---|
| rsvp          | Resource Reservation Protocol (RSVP)  |
| pim-dm        | Protocol Independent Multicast - Dense Mode (PIM-DM)  |
| pim-sm        | Protocol Independent Multicast - Sparse Mode (PIM-SM)   |
| pim-smv6      | PIM-SM version 6 (PIM-SMv6)   |
| dot1x         | IEEE 802.1X Port-Based Access Control   |
| lacp          | Link Aggregation Control Protocol (LACP)  |
| stp           | Spanning Tree Protocol (STP)  |
| rstp          | Rapid Spanning Tree Protocol (RSTP)   |
| mstp          | Multiple Spanning Tree Protocol (MSTP)  |
| imi           | Integrated Management Interface (IMI)   |
| imish         | Integrated Management Interface Shell (IMISH)   |
| epsr          | Ethernet Protection Switched Rings (EPSR)   |
| irdp          | ICMP Router Discovery Protocol (IRDP)   |
| rmon          | Remote Monitoring   |
| loopprot      | Loop Protection   |
| poe           | Power-inline (Power over Ethernet)  |
| dhcpsn        | DHCP snooping (DHPCPSN)   |
| facility      | Exclude messages from a syslog facility.  |
| <facility>    | Specify one of the following syslog facilities to exclude messages from:  |
| kern          | Kernel messages   |
| user          | Random user-level messages  |
| mail          | Mail system   |
| daemon        | System daemons  |
| auth          | Security/authorization messages   |
| syslog        | Messages generated internally by syslogd  |
| lpr           | Line printer subsystem  |
| news          | Network news subsystem  |
| uucp          | UUCP subsystem  |
| cron          | Clock daemon  |
| authpriv      | Security/authorization messages (private)   |
| ftp           | FTP daemon  |
| msgtext       | Exclude messages containing a certain text string.  |
| <text-string> | A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line. |

**Default** No log messages are excluded

**Mode** Global configuration

**Example** To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent exclude msgtext example of
irrelevant message
```

**Related commands**

- clear log permanent
- default log permanent
- log permanent
- log permanent (filter)
- log permanent size
- show log config
- show log permanent

# log permanent size

**Overview** This command configures the amount of memory that the permanent log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

Use the **no** variant of this command to return to the default.

**Syntax** `log permanent size <50-250>`  
`no log permanent size`

| Parameter                   | Description                            |
|-----------------------------|--|
| <code>&lt;50-250&gt;</code> | Size of the permanent log in kilobytes |

**Default** 50 kilobytes

**Mode** Global Configuration

**Example** To allow the permanent log to use up to 100 kilobytes of NVS, use the commands:

```
awplus# configure terminal
awplus(config)# log permanent size 100
```

To return to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# no log permanent size
```

**Related commands**

- `clear log permanent`
- `copy permanent-log`
- `default log permanent`
- `log permanent`
- `log permanent (filter)`
- `log permanent exclude`
- `show log config`
- `show log permanent`

# log-rate-limit nsm

**Overview** This command limits the number of log messages generated by the device for a given interval.

Use the **no** variant of this command to revert to the default number of log messages generated by the device of up to 200 log messages per second.

**Syntax** `log-rate-limit nsm messages <message-limit> interval <time-interval>`  
`no log-rate-limit nsm`

| Parameter                          | Description   |
|------------------------------------|---|
| <code>&lt;message-limit&gt;</code> | <code>&lt;1-65535&gt;</code><br>The number of log messages generated by the device.   |
| <code>&lt;time-interval&gt;</code> | <code>&lt;0-65535&gt;</code><br>The time period for log message generation in 1/100 seconds. If an interval of 0 is specified then no log message rate limiting is applied. |

**Default** By default, the device will allow 200 log messages to be generated per second.

**Mode** Global Configuration

**Usage notes** This log rate limiting feature constrains the rate that log messages are generated by the device. This makes sure that the device does not run out of memory from generating a lot of log messages in extreme circumstances, such as if a packet storm occurs.

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.

If you expect that there will be a lot of discarded log messages due to log rate limiting, then we recommend setting the time interval to no less than 100, which means that there would only be one log message, indicating 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
```

# log trustpoint

**Overview** This command adds one or more trustpoints to be used with the syslog application. Multiple trustpoints may be specified, or the command may be executed multiple times, to add multiple trustpoints to the application.

The **no** version of this command removes one or more trustpoints from the list of trustpoints associated with the application.

**Syntax** `log trustpoint [<trustpoint-list>]`  
`no log trustpoint [<trustpoint-list>]`

| Parameter         | Description   |
|-------------------|---|
| <trustpoint-list> | Specify one or more trustpoints to be added or deleted. |

**Default** No trustpoints are created by default.

**Mode** Global Configuration

**Usage notes** The device certificate associated with first trustpoint added to the application will be transmitted to remote servers. The certificate received from the remote server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

If no trustpoints are specified in the command, the trustpoint list will be unchanged.

If **no log trustpoint** is issued without specifying any trustpoints, then all trustpoints will be disassociated from the application.

**Example** You can add multiple trustpoints by executing the command multiple times:

```
awplus# configure terminal
awplus(config)# log trustpoint trustpoint_1
awplus(config)# log trustpoint trustpoint_2
```

Alternatively, add multiple trustpoints with a single command:

```
awplus(config)# log trustpoint trustpoint_2 trustpoint_3
```

Disassociate all trustpoints from the syslog application using the command:

```
awplus(config)# log trustpoint trustpoint_2 trustpoint_3
```

**Related commands** [log host](#)  
[show log config](#)

# log url-requests

**Overview** If URL Filtering is enabled, then by default, black list hits and issues with match criteria and list files are logged.

Use this command to enable logging of all HTTP and HTTPS URL requests (both permitted and denied) passing through the firewall.

Use the **no** variant of this command to disable extra logging of HTTP and HTTPS URL requests passing through the firewall.

**Syntax** `log url-requests`  
`no log url-requests`

**Default** Disabled by default.

**Mode** URL Filter Configuration

**Usage notes** When enabled, additional log messages for HTTP and HTTPS URL requests passing through the firewall contain the:

- URL being accessed
- IP address of the user that requested the URL

**Example** To configure logging of all HTTP and HTTPS URL requests passing through the firewall (permitted as well as denied), use the following commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# log url-requests
```

**Related commands** [url-filter](#)

**Command changes** Version 5.4.7-1.1: command added



# show connection-log events

**Overview** This command displays the configuration state (enabled or disabled) for the logging of connections passing through the firewall, as configured by the [connection-log events](#) command.

**Syntax** show connection-log events

**Mode** User Exec

**Example** To show the logging configuration state for the connections passing through the firewall, use the command:

```
awplus# show connection-log events
```

**Output** Figure 7-1: Example output from **show connection-log events**

```
awplus#show connection-log events
Log new connection events:      Disabled
Log connection end events:     Enabled
```

**Related commands** [connection-log events](#)

**Command changes** Version 5.4.7-1.1: command added.

# show counter log

**Overview** This command displays log counter information.

**Syntax** show counter log

**Mode** User Exec and Privileged Exec

**Example** To display the log counter information, use the command:

```
awplus# show counter log
```

**Output** Figure 7-2: Example output from the **show counter log** command

```
Log counters
Total Received      ..... 2328
Total Received P0   ..... 0
Total Received P1   ..... 0
Total Received P2   ..... 1
Total Received P3   ..... 9
Total Received P4   ..... 32
Total Received P5   ..... 312
Total Received P6   ..... 1602
Total Received P7   ..... 372
```

**Table 8:** Parameters in output of the **show counter log** command

| Parameter         | Description  |
|-------------------|--|
| Total Received    | Total number of messages received by the log             |
| Total Received P0 | Total number of Priority 0 (Emergency) messages received |
| Total Received P1 | Total number of Priority 1 (Alert) messages received     |
| Total Received P2 | Total number of Priority 2 (Critical) messages received  |
| Total Received P3 | Total number of Priority 3 (Error) messages received     |
| Total Received P4 | Total number of Priority 4 (Warning) messages received   |
| Total Received P5 | Total number of Priority 5 (Notice) messages received    |
| Total Received P6 | Total number of Priority 6 (Info) messages received      |
| Total Received P7 | Total number of Priority 7 (Debug) messages received     |

**Related commands** [show log config](#)

# show exception log

**Overview** This command displays the contents of the exception log.

**Syntax** show exception log

**Mode** User Exec and Privileged Exec

**Example** To display the exception log, use the command:

```
awplus# show exception log
```

**Output** Figure 7-3: Example output from the **show exception log** command on a device

```
awplus#show exception log

<date> <time> <facility>.<severity> <program[<pid>]: <message>
-----
2019 Jul 22 13:52:39 local7.debug AR1050V corehandler : Process atmfd (PID:895)
signal 11, core dumped to /flash/atmfd-arcl-main-20190705-3-1-1563760359-895.tgz
-----
```

**Output** Figure 7-4: Example output from the **show exception log** command on a device that has never had an exception occur

```
awplus#show exception log

<date> <time> <facility>.<severity> <program[<pid>]: <message>
-----
None
-----
awplus#
```

# show log

**Overview** This command displays the contents of the buffered log.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare\\_Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show log [tail [<10-250>]]`

| Parameter | Description                                   |
|-----------|---|
| tail      | Display only the latest log entries.          |
| <10-250>  | Specify the number of log entries to display. |

**Default** By default the entire contents of the buffered log is displayed.

**Mode** User Exec, Privileged Exec and Global Configuration

**Usage notes** If the optional **tail** parameter is specified, only the latest 10 messages in the buffered log are displayed. A numerical value can be specified after the **tail** parameter to select how many of the latest messages should be displayed.

The **show log** command is only available to users at privilege level 7 and above. To set a user's privilege level, use the command:

```
awplus(config)# username <name> privilege <1-15>
```

**Examples** To display the contents of the buffered log use the command:

```
awplus# show log
```

To display the 10 latest entries in the buffered log use the command:

```
awplus# show log tail 10
```

**Output** Figure 7-5: Example output from **show log**

```
awplus#show log

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
-----
2019 Jul 22 13:54:27 kern.notice awplus kernel: Linux version 4.4.6-at1
(maker@maker14-build) (gcc version 4.7.4 (crosstool-NG crosstool-ng-1.22.0) ) #1
PREEMPT Fri Jul 5 08:00:59 UTC 2019
2019 Jul 22 13:54:27 kern.notice awplus kernel: CVMSEG size: 2 cache lines (256
bytes)
2019 Jul 22 13:54:27 syslog.notice awplus syslog-ng[231]: syslog-ng starting up;
version='3.10.1'
2019 Jul 22 13:54:27 kern.notice awplus kernel: Primary instruction cache 78kB,
virtually tagged, 39 way, 16 sets, linesize 128 bytes.
2019 Jul 22 13:54:27 kern.notice awplus kernel: Primary data cache 32kB, 32-way, 8
sets, linesize 128 bytes.
2019 Jul 22 13:54:27 kern.notice awplus kernel: Kernel command line:
console=ttyS0,115200 root=/dev/r am0 releasefile=AR1050V-5.4.9-0.1.rel
bootversion=5.2.0-devel loglevel=1 mtdoops.mtddev=errlog
mtdparts=octeon_nand0:120M(user),8M(errlog) securitylevel=1
reladdr=0x8000000020010000,22cd597
2019 Jul 22 13:54:27 kern.notice awplus kernel: SCSI subsystem initialized
2019 Jul 22 13:54:27 kern.notice awplus kernel: 2 ofpart partitions found on MTD
device octeon_nand0
2019 Jul 22 13:54:27 kern.notice awplus kernel: ESP connection tracking enabled
...
```

- Related commands**
- [clear log buffered](#)
  - [copy buffered-log](#)
  - [default log buffered](#)
  - [log buffered](#)
  - [log buffered \(filter\)](#)
  - [log buffered size](#)
  - [log buffered exclude](#)
  - [show log config](#)

# show log config

**Overview** This command displays information about the logging system. This includes the configuration of the various log destinations, such as buffered, permanent, syslog servers (hosts) and email addresses. This also displays the latest status information for each log destination.

**Syntax** `show log config`

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the logging configuration use the command:

```
awplus# show log config
```

**Output** Figure 7-6: Example output from **show log config**

```
Facility: default
PKI trustpoints: example_trustpoint

Buffered log:
Status ..... enabled
Maximum size ... 100kb
Filters:
*1 Level ..... notices
  Program ..... any
  Facility ..... any
  Message text . any
  2 Level ..... informational
  Program ..... auth
  Facility ..... daemon
  Message text . any
  Statistics .... 1327 messages received, 821 accepted by filter (2016 Oct 11
10:36:16)
Permanent log:
Status ..... enabled
Maximum size ... 60kb
Filters:
  1 Level ..... error
  Program ..... any
  Facility ..... any
  Message text . any
*2 Level ..... warnings
  Program ..... dhcp
  Facility ..... any
  Message text . "pool exhausted"
  Statistics .... 1327 messages received, 12 accepted by filter (2016 Oct 11
10:36:16)
```

```
Host 10.32.16.21:
  Time offset .... +2:00
  Offset type .... UTC
  Source ..... -
  Secured ..... enabled
  Filters:
  1 Level ..... critical
    Program ..... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 1 accepted by filter (2016 Oct 11
10:36:16)
Email admin@alliedtelesis.com:
  Time offset .... +0:00
  Offset type .... Local
  Filters:
  1 Level ..... emergencies
    Program ..... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 0 accepted by filter (2016 Oct 11
10:36:16)
...
```

In the above example the '\*' next to filter 1 in the buffered log configuration indicates that this is the default filter. The permanent log has had its default filter removed, so none of the filters are marked with '\*'.

**NOTE:** Terminal log and console log cannot be set at the same time. If console logging is enabled then the terminal logging is turned off.

- Related commands**
- [show counter log](#)
  - [show log](#)
  - [show log permanent](#)

# show log external

**Overview** Use this command to display the contents of the external log, which is stored on a USB storage device.

**Syntax** `show log external [tail [<10-250>]]`

| Parameter | Description                                   |
|-----------|---|
| tail      | Display only the latest log entries.          |
| <10-250>  | Specify the number of log entries to display. |

**Mode** Global Configuration  
Privileged Exec  
User Exec

**Usage notes** If the optional **tail** parameter is specified, only the latest 10 messages in the permanent log are displayed. A numerical value can be specified after the **tail** parameter to change how many of the latest messages should be displayed.

**Example** To display the last 5 entries in the external log, use the command:

```
awplus# show log external tail 5
```

**Related commands**

- [clear log external](#)
- [default log external](#)
- [log external](#)
- [log external \(filter\)](#)
- [log external exclude](#)
- [log external rotate](#)
- [log external size](#)
- [show log config](#)
- [unmount](#)

**Command changes** Version 5.4.7-1.1: command added



# show log permanent

**Overview** This command displays the contents of the permanent log.

**Syntax** show log permanent [tail [<10-250>]]

| Parameter | Description                                   |
|-----------|---|
| tail      | Display only the latest log entries.          |
| <10-250>  | Specify the number of log entries to display. |

**Usage notes** If the optional **tail** parameter is specified only, the latest 10 messages in the permanent log are displayed. A numerical value can be specified after the **tail** parameter to change how many of the latest messages should be displayed.

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the permanent log, use the command:

```
awplus# show log permanent
```

**Output** Figure 7-7: Example output from **show log permanent**

```
awplus#show log permanent

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
-----
2014 Jun 10 09:30:09 syslog.notice syslog-ng[67]: syslog-ng starting up;
version='\2.0rc3\'
2014 Jun 10 09:30:09 auth.warning portmap[106]: user rpc not found, reverting to
user bin
2014 Jun 10 09:30:09 cron.notice crond[116]: crond 2.3.2 dillon, started, log
level 8
2014 Jun 10 09:30:14 daemon.err snmpd[181]: /flash/.configs/snmpd.conf: line 20:
Error: bad SUBTREE object
2014 Jun 10 09:30:14 user.info HSL[192]: HSL: INFO: Registering port port1.0.1
```

- Related commands**
- [clear log permanent](#)
  - [copy permanent-log](#)
  - [default log permanent](#)
  - [log permanent](#)
  - [log permanent \(filter\)](#)
  - [log permanent exclude](#)
  - [log permanent size](#)
  - [show log config](#)

# show running-config log

**Overview** This command displays the current running configuration of the Log utility.

**Syntax** `show running-config log`

**Mode** Privileged Exec and Global Configuration

**Example** To display the current configuration of the log utility, use the command:

```
awplus# show running-config log
```

**Related commands** [show log](#)  
[show log config](#)

# unmount

**Overview** Use this command to unmount an external storage device. We recommend you unmount storage devices before removing them, to avoid file corruption. This is especially important if files may be automatically written to the storage device, such as external log files or AMF backup files.

**Syntax** `unmount usb`

| Parameter | Description                     |
|-----------|---------------------------------|
| usb       | Unmount the USB storage device. |

**Mode** Privileged Exec

**Example** To unmount a USB storage device and safely remove it from the device, use the command:

```
awplus# unmount usb
```

**Related commands**

- [clear log external](#)
- [log external](#)
- [show file systems](#)
- [show log config](#)
- [show log external](#)

**Command changes** Version 5.4.7-1.1: command added

# 8

# Scripting Commands

## Introduction

**Overview** This chapter provides commands used for command scripts.

- Command List**
- [“activate”](#) on page 325
  - [“echo”](#) on page 326
  - [“wait”](#) on page 327

# activate

**Overview** This command activates a script file.

**Syntax** activate [background] <script>

| Parameter  | Description   |
|------------|---|
| background | Activate a script to run in the background. A process that is running in the background will operate as a separate task, and will not interrupt foreground processing. Generally, we recommend running short, interactive scripts in the foreground and longer scripts in the background. The default is to run the script in the foreground. |
| <script>   | The file name of the script to activate. The script is a command script consisting of commands documented in this software reference. Note that you must use either a <b>.scp</b> or a <b>.sh</b> filename extension for a valid script text file, as described below in the usage section for this command.                                  |

**Mode** Privileged Exec

**Usage notes** When a script is activated, the privilege level is set to 1 enabling User Exec commands to run in the script. If you need to run Privileged Exec commands in your script you need to add an [enable \(Privileged Exec mode\)](#) command to the start of your script. If you need to run Global Configuration commands in your script you need to add a [configure terminal](#) command after the **enable** command at the start of your script.

The **activate** command executes the script in a new shell. A [terminal length](#) shell command, such as **terminal length 0** may also be required to disable a delay that would pause the display.

A script must be a text file with a filename extension of either **.sh** or **.scp** only for the AlliedWare Plus™ CLI to activate the script file. The **.sh** filename extension indicates the file is an ASH script, and the **.scp** filename extension indicates the file is an AlliedWare Plus™ script.

**Examples** To activate a command script to run as a background process, use the command:

```
awplus# activate background test.scp
```

**Related commands**

- [configure terminal](#)
- [echo](#)
- [enable \(Privileged Exec mode\)](#)
- [wait](#)

# echo

**Overview** This command echoes a string to the terminal, followed by a blank line.

**Syntax** `echo <line>`

| Parameter                 | Description        |
|---------------------------|--------------------|
| <code>&lt;line&gt;</code> | The string to echo |

**Mode** User Exec and Privileged Exec

**Usage** This command may be useful in CLI scripts, to make the script print user-visible comments.

**Example** To echo the string `Hello World` to the console, use the command:

```
awplus# echo Hello World
```

## Output

```
Hello World
```

**Related commands** [activate](#)  
[wait](#)

# wait

**Overview** This command pauses execution of the active script for the specified period of time.

**Syntax** `wait <delay>`

| Parameter                  | Description  |
|----------------------------|--|
| <code>&lt;delay&gt;</code> | <code>&lt;1-65335&gt;</code> Specify the time delay in seconds |

**Default** No wait delay is specified by default.

**Mode** Privileged Exec (when executed from a script not directly from the command line)

**Usage notes** Use this command to pause script execution in an **.scp** (AlliedWare Plus™ script) or an **.sh** (ASH script) file executed by the [activate](#) command. The script must contain an **enable** command, because the **wait** command is only executed in the Privileged Exec mode.

**Example** See an **.scp** script file extract below that will show port counters for interface port1.0.2 over a 10 second interval:

```
enable

show interface port1.0.2

wait 10

show interface port1.0.2
```

**Related commands**

- [activate](#)
- [echo](#)
- [enable \(Privileged Exec mode\)](#)

# 9

# Interface Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure and display interfaces.

Note that this device supports only one VLAN, the default VLAN (vlan1). This VLAN does not need to be configured.

- Command List**
- “[description \(interface\)](#)” on page 329
  - “[interface \(to configure\)](#)” on page 330
  - “[ip tcp adjust-mss](#)” on page 332
  - “[ipv6 tcp adjust-mss](#)” on page 334
  - “[mru jumbo](#)” on page 336
  - “[mtu](#)” on page 337
  - “[service statistics interfaces counter](#)” on page 339
  - “[show interface](#)” on page 340
  - “[show interface brief](#)” on page 344
  - “[show interface memory](#)” on page 345
  - “[show interface status](#)” on page 347
  - “[shutdown](#)” on page 349



# description (interface)

**Overview** Use this command to add a description to a specific port or interface.

**Syntax** `description <description>`

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;description&gt;</code> | Text describing the specific interface. Descriptions can contain any printable ASCII characters (ASCII 32-126). |

**Mode** Interface Configuration

**Example** The following example uses this command to describe the device that a switch port is connected to.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# description Boardroom PC
```

**Command changes** Version 5.4.7-1.1: valid character set changed to printable ASCII characters

# interface (to configure)

**Overview** Use this command to select one or more interfaces to configure.

**Syntax** `interface <interface-list>`

| Parameter                           | Description  |
|-------------------------------------|--|
| <code>&lt;interface-list&gt;</code> | <p>The interfaces to configure. An interface-list can be:</p> <ul style="list-style-type: none"><li>• a PPP interface (e.g. ppp0)</li><li>• an Eth interface (e.g. eth1)</li><li>• vlan1</li><li>• a switchport (e.g. port1.0.4)</li><li>• a bridge interface (e.g. br0)</li><li>• a tunnel interface (e.g. tunnel0)</li><li>• a 3G cellular interface (e.g. cellular0)</li><li>• a WWAN interface (e.g. wwan0)</li><li>• the loopback interface (lo)</li><li>• a continuous range of interfaces, separated by a hyphen (e.g. ppp2-4)</li><li>• a comma-separated list (e.g. ppp0,ppp2-4). Do not mix interface types in a list.</li></ul> <p>The specified interfaces must exist.</p> |

**Usage notes** A local loopback interface is one that is always available for higher layer protocols to use and advertise to the network. Although a local loopback interface is assigned an IP address, it does not have the usual requirement of connecting to a lower layer physical entity. This lack of physical attachment creates the perception of a local loopback interface always being accessible via the network.

Local loopback interfaces can be utilized by a number of protocols for various purposes. They can be used to improve access to the device and also increase its reliability, security, scalability and protection. In addition, local loopback interfaces can add flexibility and simplify management, information gathering and filtering.

**Mode** Global Configuration

**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 PPP interface ppp0.

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)#
```

The following example shows how to enter Interface mode to configure the local loopback interface.

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)#
```

The following example shows how to enter Interface mode to configure bridge br2.

```
awplus# configure terminal
awplus(config)# interface br2
awplus(config-if)#
```

**Related commands**

- [ip address \(IP Addressing and Protocol\)](#)
- [show interface](#)
- [show interface brief](#)

# ip tcp adjust-mss

**Overview** Use this command to set the Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

**Syntax** `ip tcp adjust-mss {<mss-size>|pmtu}`  
`no ip tcp adjust-mss`

| Parameter                     | Description  |
|-------------------------------|--|
| <code>&lt;mss-size&gt;</code> | <code>&lt;64-1460&gt;</code> Specifies the MSS size in bytes.          |
| <code>pmtu</code>             | Adjust TCP MSS automatically with respect to the MTU on the interface. |

**Default** The default setting allows a TCP server or a TCP client to set the MSS value for itself.

**Mode** Interface Configuration

**Usage notes** When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel
- VLAN

**Examples** To configure an MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ip tcp adjust-mss 1452
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip tcp adjust-mss
```

**Related  
commands**

[mtu \(PPP\)](#)  
[show interface](#)  
[show interface \(PPP\)](#)

**Command  
changes**

Version 5.4.8-2.1: interface tunnel example added

# ipv6 tcp adjust-mss

**Overview** Use this command to set the IPv6 Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

**Syntax** `ipv6 tcp adjust-mss {<mss-size>|pmtu}`  
`no ipv6 tcp adjust-mss`

| Parameter                     | Description  |
|-------------------------------|--|
| <code>&lt;mss-size&gt;</code> | <code>&lt;64-1460&gt;</code> Specifies the MSS size in bytes.          |
| <code>pmtu</code>             | Adjust TCP MSS automatically with respect to the MTU on the interface. |

**Default** The default setting allows a TCP server or a TCP client to set the MSS value for itself.

**Mode** Interface Configuration

**Usage notes** When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel
- VLAN

**Examples** To configure an IPv6 MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To configure an IPv6 MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To adjust IPv6 TCP MSS automatically with respect to the MTU on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ipv6 tcp adjust-mss pmtu
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 tcp adjust-mss
```

**Related  
commands**

[mtu \(PPP\)](#)  
[show interface](#)  
[show interface \(PPP\)](#)

**Command  
changes**

Version 5.4.8-2.1: interface tunnel example added

# mru jumbo

**Overview** Use this command to enable the device to forward jumbo frames. For more information, see the [Switching\\_Feature Overview and Configuration Guide](#).

When jumbo frame support is enabled, the maximum size of packets that the device can forward is 9688 bytes of payload.

Use the **no** variant of this command to remove jumbo frame support, and restore the default MRU size (1500 bytes) for switch ports.

**NOTE:**

*The figure above 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 (to 1522 bytes in the default case).*

**Syntax** mru jumbo  
no mru

**Default** By default, jumbo frame support is not enabled.

**Mode** Interface Configuration for switch ports.

**Usage notes** Note that [show interface](#) output will only show MRU size for switch ports.

We recommend limiting the number of ports with jumbo frames support enabled to two.

**Examples** To enable the device to forward jumbo frames on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# mru jumbo
```

To remove the jumbo frame support, and therefore restore the MRU size of 1500 bytes on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no mru
```

**Related commands** [show interface](#)



## mtu

**Overview** Use this command to set the Maximum Transmission Unit (MTU) size for interfaces, where MTU is the maximum packet size that interfaces can transmit. The MTU size setting is applied to both IPv4 and IPv6 packet transmission.

Use the **no** variant of this command to remove a previously specified Maximum Transmission Unit (MTU) size, and restore the default MTU size. For example the VLAN interface default is 1500 bytes.

**Syntax** `mtu <68-1582>`  
`no mtu`

**Default** The default MTU size, for example 1500 bytes for VLAN interfaces.

**Mode** Interface Configuration

**Usage notes** If a device receives an IPv4 packet for Layer 3 switching to another interface with an MTU size smaller than the packet size, and if the packet has the **'don't fragment'** bit set, then the device will send an ICMP **'destination unreachable'** (3) packet type and a **'fragmentation needed and DF set'** (4) code back to the source. For IPv6 packets bigger than the MTU size of the transmitting interface, an ICMP **'packet too big'** (ICMP type 2 code 0) message is sent to the source.

You can set a feasible MTU value on the following interfaces:

- PPP
- Ethernet
- Tunnel
- VLAN

Note that you cannot configure MTU on bridge interfaces. The MTU of the bridge interface is determined by the member interface of the bridge which has the lowest MTU. For example, if you attach eth1 with MTU 1200, ppp1 with MTU 1400, and vlan1 with MTU 1500 to a bridge interface, the MTU for that interface will be 1200.

Note that `show interface` output will only show MTU size for VLAN interfaces.

**Examples** To configure an MTU size of 1500 bytes on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# mtu 1500
```

To configure an MTU size of 1500 bytes for tunnel "tunnel2", use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# mtu 1500
```

To restore the MTU size to the default MTU size of 1500 bytes on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no mtu
```

**Related commands** [show interface](#)

# service statistics interfaces counter

**Overview** Use this command to enable the interface statistics counter.  
Use the **no** variant of this command to disable the interface statistics counter.

**Syntax** service statistics interfaces counter  
no service statistics interfaces counter

**Default** The interface statistics counter is enabled by default.

**Mode** Global Configuration

**Example** To enable the interface statistics counter, use the following commands:

```
awplus# configure terminal  
awplus(config)# service statistics interfaces counter
```

To disable the interface statistics counter, use the following commands:

```
awplus# configure terminal  
awplus(config)# no service statistics interfaces counter
```

**Command changes** Version 5.4.7-2.1: command added

# show interface

**Overview** Use this command to display interface configuration and status.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show interface [<interface-list>]`

| Parameter                           | Description   |
|-------------------------------------|---|
| <code>&lt;interface-list&gt;</code> | <p>The interfaces or ports to display. An interface-list can be:</p> <ul style="list-style-type: none"><li>• a PPP interface (e.g. ppp0)</li><li>• an Eth interface (e.g. eth1)</li><li>• vlan1</li><li>• a switchport (e.g. port1.0.4)</li><li>• a bridge interface (e.g. br0)</li><li>• a tunnel interface (e.g. tunnel0)</li><li>• a 3G cellular interface (e.g. cellular0)</li><li>• a WWAN interface (e.g. wwan0)</li><li>• the loopback interface (lo)</li><li>• a continuous range of interfaces, separated by a hyphen (e.g. ppp2-4)</li><li>• a comma-separated list (e.g. ppp0,ppp2-4). Do not mix interface types in a list.</li></ul> <p>The specified interfaces must exist.</p> |

**Mode** User Exec and Privileged Exec

**Usage notes** Note that the output displayed with this command will show MTU (Maximum Transmission Unit) size for VLAN interfaces, and MRU (Maximum Received Unit) size for switch ports.

**Example** To display configuration and status information for all interfaces, use the command:

```
awplus# show interface
```

Figure 9-1: Example output from the **show interface** command

```
awplus#show interface
Interface port1.0.1
  Link is UP, administrative state is UP
  Hardware is Ethernet, address is 0000.cd38.026c
  index 5001 metric 1 mru 1500
  current duplex full, current speed 1000, current polarity mdix
  configured duplex auto, configured speed auto, configured polarity auto
  <UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  input packets 2927667, bytes 224929311, dropped 0, multicast packets 1242629
  output packets 378084, bytes 54372424, multicast packets 1, broadcast packets 10
  input average rate : 30 seconds 5.19 Kbps, 5 minutes 8.16 Kbps
  output average rate: 30 seconds 6.04 Kbps, 5 minutes 73.89 Kbps
  input peak rate 268.60 Kbps at 2018/04/10 17:46:43
  output peak rate 6.81 Mbps at 2018/04/10 18:15:44
  Time since last state change: 7 days 01:58:10
  ...
```

To display configuration and status information for the loopback interface lo, use the command:

```
awplus# show interface lo
```

Figure 9-2: Example output from the **show interface lo** command

```
awplus#show interface lo
Interface lo
  Link is UP, administrative state is UP
  Hardware is Loopback
  index 1 metric 1
  <UP,LOOPBACK,RUNNING>
  VRF Binding: Not bound
  SNMP link-status traps: Disabled
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
  Time since last state change: 8 days 19:41:47
```

To display configuration and status information for interface vlan1, use the command:

```
awplus# show interface vlan1
```

Figure 9-3: Example output from the **show interface vlan1** command

```
awplus#show interface vlan1
Interface vlan1
  Link is UP, administrative state is UP
  Hardware is VLAN, address is 0000.cd38.026c
  IPv4 address 192.168.1.1/24 broadcast 192.168.1.255
  index 301 metric 1 mtu 1500
  arp ageing timeout 300
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  SNMP link-status traps: Disabled
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
  input packets 0, bytes 0, dropped 0, multicast packets 0
  output packets 9, bytes 612, multicast packets 0, broadcast packets 0
  input average rate : 30 seconds 0 bps, 5 minutes 0 bps
  output average rate: 30 seconds 0 bps, 5 minutes 0 bps
  output peak rate 140 bps at 2018/04/10 16:40:56
  Time since last state change: 8 days 19:09:19
```

To display configuration and status information for br1, use the command:

```
awplus# show interface br1
```

```
awplus#show interface br1
Interface br1
  Link is UP, administrative state is UP
  Hardware is Bridge
  IPv6 address fe80::200:cdff:fe38:f7/64
  index 33555969 metric 1
  MAC ageing time 300
  <UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  input packets 1328, bytes 143605, dropped 0, multicast packets 0
  output packets 1847, bytes 218999, multicast packets 1 broadcast packets 3
  input average rate : 30 seconds 3.00 Kbps, 5 minutes 1.02 Kbps
  output average rate: 30 seconds 5.32 Kbps, 5 minutes 2.06 Kbps
  input peak rate 8.19 Kbps at 2017/11/13 05:09:59
  output peak rate 17.05 Kbps at 2017/11/13 05:11:23
  Time since last state change: 0 days 00:00:09
```

To display configuration and status information for eth1, use the command:

```
awplus# show interface eth1
```

Figure 9-4: Example output from the **show interface eth1** command:

```
awplus#show interface eth1
Interface eth1
  Link is DOWN, administrative state is UP
  Hardware is Ethernet, address is 0000.cd38.026a
  index 12 metric 1 mtu 1500
  configured duplex auto, configured speed auto, configured polarity auto
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
  input packets 0, bytes 0, dropped 0, multicast packets 0
  output packets 11, bytes 5848
  input average rate : 30 seconds 0 bps, 5 minutes 0 bps
  output average rate: 30 seconds 0 bps, 5 minutes 0 bps
  output peak rate 2.48 Kbps at 2018/04/10 18:22:14
  Time since last state change: 7 days 22:56:59
```

**Related commands** [mru jumbo](#)  
[mtu](#)

[show interface brief](#)

**Command changes** Version 5.4.7-2.1: average rate and peak rate added to output

# show interface brief

**Overview** Use this command to display brief interface, configuration, and status information, including provisioning information.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show interface brief`

**Mode** User Exec and Privileged Exec

**Output** Figure 9-5: Example output from **show interface brief**

```
awplus#show interface brief
Interface          Status           Protocol
port1.0.1         admin up        down
port1.0.2         admin up        down
port1.0.3         admin up        down
port1.0.4         admin up        down
...
eth1              admin up        down
lo               admin up        running
vlan1            admin up        down
ppp1             admin up        down
```

Table 9-1: Parameters in the output of **show interface brief**

| Parameter | Description   |
|-----------|---|
| Interface | The name or type of interface.  |
| Status    | The administrative state. This can be either <b>admin up</b> or <b>admin down</b> .       |
| Protocol  | The link state. This can be either <b>down</b> , <b>running</b> , or <b>provisioned</b> . |

**Related commands** [show interface](#)  
[show interface memory](#)



# show interface memory

**Overview** This command displays the shared memory used by either all interfaces, or the specified interface or interfaces. The output is useful for diagnostic purposes by Allied Telesis authorized service personnel.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show interface memory`  
`show interface <port-list> memory`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;port-list&gt;</code> | Display information about only the specified port or ports. The port list can be: <ul style="list-style-type: none"><li>• an Eth port (e.g. eth1)</li><li>• a switchport (e.g. port1.0.4)</li><li>• a continuous range of ports separated by a hyphen (e.g. port1.0.1-1.0.4)</li><li>• a comma-separated list (e.g. port1.0.1,port1.0.3-1.0.4). Do not mix port types in the same list.</li></ul> |

**Mode** User Exec and Privileged Exec

**Example** To display the shared memory used by all interfaces, use the command:

```
awplus# show interface memory
```

To display the shared memory used by port1.0.1 and port1.0.3 to port1.0.4, use the command:

```
awplus# show interface port1.0.1,port1.0.3-port1.0.4 memory
```

**Output** Figure 9-6: Example output from the **show interface memory** command

```
awplus#show interface memory
Vlan blocking state shared memory usage
-----
Interface    shmid      Bytes Used    natch      Status
port1.0.1    294921     512           1
port1.0.2    491535     512           1
port1.0.3    458766     512           1
...
eth1         393228     512           1
lo          360459     512           1
```

Figure 9-7: Example output from **show interface <port-list> memory** for a list of interfaces

```
awplus#show interface port1.0.1,port1.0.3-port1.0.4 memory
Vlan blocking state shared memory usage
-----
Interface      shmid      Bytes Used  natch      Status
port1.0.1      589842     512         1          1
port1.0.3      688149     512         1          1
port1.0.4      327690     512         1          1
```

**Related  
commands**

- [show interface brief](#)
- [show interface status](#)
- [show interface switchport](#)

# show interface status

**Overview** Use this command to display the status of the specified interface or interfaces. Note that when no interface or interfaces are specified then the status of all interfaces on the device are shown.

**Syntax** `show interface [<port-list>] status`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;port-list&gt;</code> | The ports to display information about. The port list can be: <ul style="list-style-type: none"><li>• an Eth port (e.g. eth1)</li><li>• a switchport (e.g. port1.0.4)</li><li>• a continuous range of ports separated by a hyphen (e.g. port1.0.1-1.0.4)</li><li>• a comma-separated list (e.g. port1.0.1,port1.0.3-1.0.4). Do not mix port types in the same list.</li></ul> |

**Examples** To display the status of port1.0.1 to port1.0.3, use the commands:

```
awplus# show interface port1.0.1-port1.0.3 status
```

**Table 10:** Example output from the `show interface <port-list> status` command

```
awplus#show interface port1.0.1-port1.0.3 status
```

| Port      | Name | Status     | Vlan | Duplex | Speed | Type       |
|-----------|------|------------|------|--------|-------|------------|
| port1.0.1 |      | notconnect | 1    | auto   | auto  | 1000BASE-T |
| port1.0.2 |      | notconnect | 1    | auto   | auto  | 1000BASE-T |
| port1.0.3 |      | notconnect | 1    | auto   | auto  | 1000BASE-T |

To display the status of all ports, use the commands:

```
awplus# show interface status
```

**Table 11:** Example output from the `show interface status` command

```
awplus#show interface status
```

| Port      | Name        | Status    | Vlan  | Duplex | Speed  | Type       |
|-----------|-------------|-----------|-------|--------|--------|------------|
| port1.0.1 | Trunk_Net   | connected | trunk | a-full | a-1000 | 1000BaseTX |
| port1.0.2 | Access_Net1 | connected | 1     | full   | 1000   | 1000BaseTX |
| port1.0.3 | Access_Net1 | disabled  | 1     | auto   | auto   | 1000BaseTX |
| ...       |             |           |       |        |        |            |

**Table 12:** Parameters in the output from the **show interface status** command

| Parameter | Description  |
|-----------|--|
| Port      | Name/Type of the interface.  |
| Name      | Description of the interface.  |
| Status    | The administrative and operational status of the interface; one of: <ul style="list-style-type: none"> <li>disabled: the interface is administratively down.</li> <li>connect: the interface is operationally up.</li> <li>notconnect: the interface is operationally down.</li> </ul>   |
| Vlan      | VLAN type or VLAN IDs associated with the port: <ul style="list-style-type: none"> <li>When the port is a switchport in access mode, it displays the VLAN ID. This device supports the default VLAN only, vlan1.</li> <li>When the port is an Eth port, it displays <b>none</b>: there is no VLAN associated with it.</li> </ul> |
| Duplex    | The actual duplex mode of the interface, preceded by <b>a-</b> if it has autonegotiated this duplex mode. If the port is disabled or not connected, it displays the configured duplex setting.   |
| Speed     | The actual link speed of the interface, preceded by <b>a-</b> if it has autonegotiated this speed. If the port is disabled or not connected, it displays the configured speed setting.   |
| Type      | The type of interface, e.g. 1000BaseTX.  |

**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** To shut down port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# shutdown
```

To bring up port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no shutdown
```

To shut down vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# shutdown
```

To bring up vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no shutdown
```

# 10

# USB Cellular Modem Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure USB Cellular Modems.

For more information, see the [USB Cellular Modem Feature Overview and Configuration Guide](#).

- Command List**
- [“apn”](#) on page 351
  - [“chat-script”](#) on page 353
  - [“cid”](#) on page 354
  - [“encapsulation ppp”](#) on page 355
  - [“show cellular”](#) on page 356
  - [“show system usb”](#) on page 359
  - [“usb mode-switch”](#) on page 361

# apn

**Overview** Use this command to set the Access Point Name (APN) to use to connect to a 3G serial cellular network.

Use the **no** variant of this command to unset the APN.

**Syntax** `apn <access-point-name>`  
`no apn`

| Parameter                              | Description   |
|--|---|
| <code>&lt;access-point-name&gt;</code> | The APN to use to connect to a cellular network (for example, <code>www.example.com</code> ). |

**Default** No APN is set

**Mode** Interface Configuration (Cellular)

**Usage notes** The APN has to be set in order to initiate the cellular network connection. Some mobile network operators do not require a specific APN to be specified, in this case any APN can be used.

**Examples** To set the APN to `www.example.com` for a cellular interface, use the commands:

```
awplus# configure terminal
awplus(config)# int cellular0
awplus(config-if)# apn www.example.com
```

**Output** Figure 10-1: Example output from the **apn** command

```
awplus#configure terminal
awplus(config)#int cellular0
awplus(config-if)#apn www.example.com
```

To unset the APN, use the commands:

```
awplus# configure terminal
awplus(config)# int cellular0
awplus(config-if)# no apn
```

**Output** Figure 10-2: Example output from the **no apn** command

```
awplus#configure terminal
awplus(config)#int cellular0
awplus(config-if)#no apn
```

**Related commands** [chat-script](#)

show cellular  
show system usb  
usb mode-switch



# chat-script

**Overview** Use this command to set a chat-script, instead of the default chat-script, to connect to a 3G serial cellular network.

Use the **no** variant of this command to set the chat-script back to the default.

**Syntax** `chat-script <file-name>`  
`no chat-script`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;file-name&gt;</code> | The path to the chat-script file (this file has to have a ".chat" extension). |

**Default** The default chat-script is a built-in chat-script that in most cases is sufficient for connecting to a cellular network.

**Mode** Interface Configuration (Cellular)

**Usage notes** The chat-script file must have the file extension ".chat". The chat-script consists of a sequence of expect-send pairs of strings. The send strings are AT (Hayes) commands. Any occurrence of the string \$APN in the chat-script will be substituted with the Access Point Name (APN) configured on a cellular interface.

**Examples** To use a non-default chat-script, "connect.chat", use the commands:

```
awplus# configure terminal
awplus(config)# interface cellular0
awplus(config-if)# #chat-script connect.chat
```

To use the default chat-script, use the commands:

```
awplus# configure terminal
awplus(config)# interface cellular0
awplus(config-if)# #no chat-script
```

**Related commands**

- [apn](#)
- [cid](#)
- [show cellular](#)
- [show system usb](#)
- [usb mode-switch](#)

# cid

**Overview** Use this command to set the PDP Context-ID (CID). The customer information in the CID is used to connect to a 3G cellular network.

Use the **no** variant of this command to set the CID back to the default value of 1.

**Syntax** `cid <context-id>`  
`no cid`

| Parameter                       | Description  |
|---------------------------------|--|
| <code>cid</code>                | Context ID (CID) includes identifying information about the mobile customer.<br>For example, the PDP Contexts include the Context-ID that contains the following information:<br>Type, APN, Address, Header Compression, and Status. |
| <code>&lt;context-id&gt;</code> | The Context-ID is a number from the range 1 to 10.   |

**Default** Context-ID is set to 1

**Mode** Interface Configuration (cellular)

**Usage notes** Some cellular modems may have elements of the CID that are read-only.  
Use this command to change the CID instead of using a custom chat-script.

**Examples** To set the Context ID to 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface cellular0
awplus(config-if)# cid 2
```

To set the Context ID back to the default value of 1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface cellular0
awplus(config-if)# no cid
```

**Related commands** [apn](#)  
[chat-script](#)  
[show cellular](#)

**Command changes** Version 5.4.9-2.1: command added

# encapsulation ppp

**Overview** Use this command to enable PPP encapsulation and create one or more PPP interfaces over Ethernet or a cellular interface.

Use the **no** variant of this command to disable PPP encapsulation and remove the specified PPP interface.

**Syntax** `encapsulation ppp <index>`  
`no encapsulation ppp <index>`

| Parameter | Description  |
|-----------|--|
| <index>   | The PPP interface index number in the range from 0 to 255. |

**Default** No PPP encapsulation or interfaces are configured by default.

**Mode** Interface Configuration mode for an Ethernet interface (e.g. **interface eth1**), or an Ethernet sub-interface (e.g. **interface eth1.1**), or a cellular interface (e.g. **interface cellular0**).

**Examples** To configure a PPP interface with index 0 for Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# encapsulation ppp 0
```

To shut down the ppp0 interface and remove it from Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# shutdown
awplus(config-if)# interface eth1
awplus(config-if)# no encapsulation ppp 0
```

**Related commands** [ppp service-name \(PPPoE\)](#)  
[show interface \(PPP\)](#)

# show cellular

**Overview** Use this command to display status information about 3G serial USB cellular modems currently plugged into your AR-Series Firewall.

**Syntax** `show cellular <cellular-interface-name>`

| Parameter                                    | Description  |
|--|--|
| <code>&lt;cellular-interface-name&gt;</code> | Specify the name of a cellular interface. This option displays status information for the cellular modem associated with that interface. |

**Default** None

**Mode** Privileged Exec

**Usage notes** If a cellular interface is specified, then the command only shows information for the cellular modem associated with that interface. Different vendors, and models of cellular modems often provide different sets of information:

- Vendor-specific information will not be displayed if the information is unable to be obtained from the cellular modem.
- For information that is common to most cellular modems, "(unknown)" will be displayed if the information was not obtained successfully.

**Examples** To show status information about all cellular modems, use the command:

```
awplus# show cellular
```

**Output** Figure 10-3: Example output from **show cellular**

```
awplus#show cellular
Interface cellular0
  Manufacturer: huawei
  Model ID: E1762
  Revision ID: 11.126.10.00.74
  Serial ID: 351553036840711
  IMSI: 530011104647258
  Signal Quality:
    RSSI: -71 dBm
    Bit Error Rate: (unknown)
  Service Center Address:
    Phone Number: +6421600600
    Number Type: International
  GPRS Mobile Station Class: Class A
  Serial Port Configuration:
    Baud rate: 115200
    Character Format: 8-N-1
    Parity: Space
```

```
Terminal Equipment Character Set: IRA
Cable interface DTE-DCE local flow control:
  To DTE: RTS
  To DCE: CTS
System Time: 1980/01/06,03:37:39
GPRS Network Registration Status: Registered, home network
PIN Request Status: READY
Functionality Level: Full functionality (power-saving disabled)
Facility Lock Status:
  SIM card lock: Not active
  SIM fixed dialling memory feature: Not active
  Network personalization: Not active
  Network subset personalization: Not active
  Service provider personalization: Not active
  Corporate personalization: Not active
  Lock phone to first SIM card: Not active
Call Mode: Single mode
Wireless Data Service: 3GPP systems (GERAN, UTRAN and E-UTRAN)
GPRS Service Status: Mobile station is attached to a GPRS service
Dialling Number Type: National
Bearer Service Type:
  Autobauding: Enabled
  Service: Data circuit asynchronous (UDI or 3.1 kHz modem)
  Connection Element: Non-transparent
Automatic time and time zone update via NITS: Not enabled
PPP support between TE and MT: Supported
Last Error Report: No cause information available
PLMN selection method: User controlled PLMN selected from Access Technology
PDP Contexts:
  Context ID: 1
  Type: IP
  APN: www.vodafone.net.nz
  Address: 0.0.0.0
  Header Compression: Off
  Status: Not active
  Primary DNS: 0.0.0.0
  Secondary DNS: 0.0.0.0
  Diagnostic mode baud rate: 115200
  TE-DCE baud rate: 115200
  Tolerance to long delays in PDP call setup: Enabled
  Hardware Version: CD25TCPV
System Info:
  System Service State: Valid service
  System Service Domain: CS and PS service
  Roaming Status: Not roaming
  System Mode: WCDMA mode
  SIM card state: Valid USIM card state
  System Sub-mode: WCDMA mode
System Config:
  Supported System Mode: Auto-select
  Network Acquisition Order: WCDMA, then GSM
  Service Domain Support: CS and PS
Card-Lock:
  Lock Status: Unlock code does not need to be provided
  Remaining Unlock Attempts: 10
  PLMN ID of the operator who has locked this device: None
```

```
Signal Strength:
  RSSI (dBm): -64
  ECIO (dBm): -5
  RSCP (dBm): -69
ICCID: 984610411061462785F5
Software Version: E1762 11.126.10.00.74,CD25TCPV,Ver.B
HSUPA status: Enabled
HSDPA status: Enabled
Card Mode: USIM
Device Mode:
  Mode ID: 20
  Port Modes:
    Port 0: MDM
    Port 1: NDIS
    Port 2: DIAG
    Port 3: PCUI
    Port 4: CDROM
Data Service Traffic:
  Last Connection Time (s): 5134
  Last Bytes Transmitted: 0
  Last Bytes Received: 168
  Total Connection Time (s): 64354
  Total Bytes Transmitted: 910
  Total Bytes Received: 3168
PIN Status:
  Status: READY
  Remaining input attempts:
    PUK: 10
    PIN: 3
    PUK2: 10
    PIN2: 3
```

To show status information about the cellular modem associated with interface 'cellular0' only, use the command:

```
awplus# show cellular cellular0
```

**Related  
commands**

[apn](#)  
[chat-script](#)  
[show system usb](#)  
[usb mode-switch](#)

# show system usb

**Overview** Use this command to display technical information about connected USB devices.

**Syntax** `show system usb [detail]`

| Parameter | Description  |
|-----------|--|
| detail    | This option provides greater detail about the USB device, such as descriptors for the device, configuration and Interface. |

**Default** None

**Mode** Privileged Exec

**Examples** To show information about USB devices connected to your AR-Series Firewall, use the command:

```
awplus# show system usb
```

**Output** Figure 10-4: Example output from **show system usb**

```
awplus#show system usb
Bus 001 Device 003: ID 12d1:140c Huawei Technologies Co., Ltd. E180v modem
```

To show greater detail of information about USB devices connected to your AR-Series Firewall, use the command:

```
awplus# show system usb detail
```

**Output** Figure 10-5: Example output from **show system usb detail**

```
awplus#show system usb detail

Bus 001 Device 002: ID 12d1:1001 Huawei Technologies Co., Ltd. E169/E620/E800 HS
DPA Modem
Device Descriptor:
  bLength                18
  bDescriptorType        1
  bcdUSB                  2.00
  bDeviceClass            0 (Defined at Interface level)
  bDeviceSubClass        0
  bDeviceProtocol        0
  bMaxPacketSize0       64
```

```
idVendor      0x12d1 Huawei Technologies Co., Ltd.
idProduct     0x1001 E169/E620/E800 HSDPA Modem
bcdDevice     0.00
iManufacturer 3 HUAWEI Technology
iProduct      2 HUAWEI Mobile
iSerial       0
bNumConfigurations 1
Configuration Descriptor:
  bLength      9
  bDescriptorType 2
  wTotalLength 85
  bNumInterfaces 3
  bConfigurationValue 1
  iConfiguration 1 Huawei Configuration
  bmAttributes 0xe0
    Self Powered
    Remote Wakeup
  MaxPower     500mA
Interface Descriptor:
  bLength      9
  bDescriptorType 4
  bInterfaceNumber 0
  bAlternateSetting 0
  bNumEndpoints 3
  bInterfaceClass 255 Vendor Specific Class
  bInterfaceSubClass 255 Vendor Specific Subclass
  bInterfaceProtocol 255 Vendor Specific Protocol
  iInterface    0
...

```

- Related commands**
- [apn](#)
  - [chat-script](#)
  - [show cellular](#)
  - [usb mode-switch](#)



# usb mode-switch

**Overview** Use this command to map a specific USB device to a mode-switch configuration file.

The **no** variant of this command removes the configuration corresponding to a specific ID.

**Syntax** `usb mode-switch id <1-16> vendor-id <vendor-id> product-id <product-id> [manufacturer <manufacturer>|product <product>|serial <serial>|vendor <vendor>|model <model>|revision <revision>] file <file-name>`  
`no usb mode-switch id <1-16>`

| Parameter      | Description  |
|----------------|--|
| id             | mode switch configuration ID.  |
| <1-16>         | Configuration ID number (from 1 through 16).   |
| vendor-id      | Specify the USB device's vendor ID.  |
| <vendor-id>    | 4 digit hexadecimal value representing the device's vendor ID.                               |
| product-id     | Specify the USB device's product ID.   |
| <product-id>   | 4 digit hexadecimal value representing the device's product ID.                              |
| manufacturer   | Specify the USB manufacturer descriptor.   |
| <manufacturer> | All or part of the USB manufacturer string descriptor (with spaces replaced by underscores). |
| product        | Specify the USB product descriptor.  |
| <product>      | All or part of the USB product string descriptor (with spaces replaced by underscores).      |
| serial         | Specify the USB serial descriptor.   |
| <serial>       | All or part of the USB serial string descriptor (with spaces replaced by underscores).       |
| vendor         | Specify the SCSI vendor descriptor.  |
| <vendor>       | All or part of the SCSI model descriptor (with spaces replaced by underscores).              |
| model          | Specify the SCSI model descriptor.   |
| <model>        | All or part of the SCSI revision descriptor (with spaces replaced by underscores).           |
| revision       | Specify the SCSI revision descriptor.  |
| <revision>     | All or part of the SCSI revision descriptor (with spaces replaced by underscores).           |

| Parameter                 | Description   |
|---------------------------|---|
| <code>file</code>         | Specify the mode switch config file to be used instead of the default when the target device is inserted. |
| <code>&lt;file&gt;</code> | Mode switch configuration file URL with extension <code>.conf</code> .                                    |

**Default** Some USB devices will use a default mode switch configuration file if one is not specified.

**Mode** Global Configuration

**Usage notes** Some USB devices must be explicitly told to switch to a compatible mode. The **usb mode-switch** command does this by matching on a target device by its USB vendor and product IDs, and executing a specified configuration file.

Additional parameters can be defined which specify other USB and SCSI descriptors. These are useful if there are multiple devices that have the same product and vendor IDs, but differ in the other parameters. The mode switch configuration files must have the extension `".conf"`.

**Examples** To add a mode switch configuration for a USB device, use the commands:

```
awplus# configure terminal
awplus(config)# usb mode-switch id 1 vendor-id 12d1 product-id
140c manufacturer HUAWEI file switch.conf
```

To remove a mode switch configuration for a USB device, use the commands:

```
awplus# configure terminal
awplus(config)# no usb mode-switch id 1
```

**Related commands**

- [apn](#)
- [chat-script](#)
- [show cellular](#)
- [show system usb](#)
- [usb mode-switch](#)

# Part 2: Interfaces and Layer 2

# 11

# Switching Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure switching.

For more information, see the [Switching Feature Overview and Configuration Guide](#).

- Command List**
- “backpressure” on page 366
  - “clear mac address-table dynamic” on page 368
  - “clear mac address-table static” on page 369
  - “clear port counter” on page 370
  - “debug platform packet” on page 371
  - “duplex” on page 373
  - “flowcontrol (switch port)” on page 374
  - “linkflap action” on page 376
  - “mac address-table acquire” on page 377
  - “mac address-table ageing-time” on page 378
  - “mac address-table static” on page 379
  - “polarity” on page 380
  - “show debugging platform packet” on page 381
  - “show flowcontrol interface” on page 382
  - “show interface err-disabled” on page 383
  - “show interface switchport” on page 384
  - “show mac address-table” on page 385
  - “show platform” on page 387

- [“show platform port”](#) on page 389
- [“show storm-control”](#) on page 391
- [“speed”](#) on page 392
- [“storm-control level”](#) on page 394
- [“undebbug platform packet”](#) on page 395

# backpressure

**Overview** This command provides a method of applying flow control to ports running in half duplex mode. The setting will only apply when the link is in the half-duplex state.

You can disable backpressure on an interface using the **off** parameter or the **no** variant of this command.

**Syntax** `backpressure {on|off}`  
`no backpressure`

| Parameters | Description                        |
|------------|------------------------------------|
| on         | Enables half-duplex flow control.  |
| off        | Disables half-duplex flow control. |

**Default** Backpressure is turned off by default. You can determine whether an interface has backpressure enabled by viewing the running-config output; **backpressure on** is shown for interfaces if this feature is enabled.

**Mode** Interface Configuration

**Usage notes** The backpressure feature enables half duplex Ethernet ports to control traffic flow during congestion by preventing further packets arriving. Back pressure utilizes a pre-802.3x mechanism in order to apply Ethernet flow control to switch ports that are configured in the half duplex mode.

The flow control applied by the [flowcontrol \(switch port\)](#) command operates only on full-duplex links, whereas back pressure operates only on half-duplex links.

If a port has insufficient capacity to receive further frames, the device will simulate a collision by transmitting a CSMA/CD jamming signal from this port until the buffer empties. The jamming signal causes the sending device to stop transmitting and wait a random period of time, before retransmitting its data, thus providing time for the buffer to clear. Although this command is only valid for switch ports operating in half-duplex mode the remote device (the one sending the data) can be operating in the full duplex mode.

To see the currently-negotiated duplex mode for ports whose links are up, use the command [show interface](#). To see the configured duplex mode (when different from the default), use the command [show running-config](#).

**Examples** To enable back pressure flow control on interfaces `port1.0.1-port1.0.2` enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# backpressure on
```

To disable back pressure flow control on interface `port1.0.2` enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# backpressure off
```

**Validation  
Commands**    `show running-config`  
                  `show interface`

**Related  
commands**    `duplex`

# clear mac address-table dynamic

**Overview** Use this command to clear the filtering database of all entries learned for a selected MAC address, a switch port interface or VLAN1.

**Syntax** `clear mac address-table dynamic`  
`[address <mac-address>|interface <port>/vlan 1]`

| Parameter  | Description   |
|--|---|
| <code>address</code><br><code>&lt;mac-address&gt;</code> | Specify a MAC (Media Access Control) address to be cleared from the filtering database, in the format HHHH.HHHH.HHHH.   |
| <code>interface &lt;port&gt;</code>                      | Specify a switch port to be cleared from the filtering database. The port can be: <ul style="list-style-type: none"><li>• a switchport (e.g. port1.0.4)</li></ul> |
| <code>vlan 1</code>                                      | Specify VLAN1 to be cleared from the filtering database.  |

**Mode** Privileged Exec

**Usage notes** Use this command with options to clear the filtering database of all entries learned for a given MAC address, interface or VLAN. Use this command without options to clear any learned entries.

**Examples** This example shows how to clear all dynamically learned filtering database entries.

```
awplus# clear mac address-table dynamic
```

This example shows how to clear all dynamically learned filtering database entries when learned through device operation for the MAC address 0000.5E00.5302.

```
awplus# clear mac address-table dynamic address 0000.5E00.5302
```

**Related commands** [clear mac address-table static](#)  
[show mac address-table](#)



# clear mac address-table static

**Overview** Use this command to clear the filtering database of all statically configured entries for a selected MAC address, interface, or VLAN.

**Syntax** `clear mac address-table static [address <mac-address>|interface <port>|vlan 1]`

| Parameter                | Description  |
|--------------------------|--|
| address<br><mac-address> | Specify a MAC (Media Access Control) address to be cleared from the filtering database, in the format HHHH.HHHH.HHHH.  |
| interface <port>         | Specify the port from which statically configured entries are to be cleared. The port can be <ul style="list-style-type: none"><li>a switchport (e.g. port1.0.4)</li></ul> |
| vlan 1                   | Specify VLAN1 to be cleared from the filtering database.   |

**Mode** Privileged Exec

**Usage notes** Use this command with options to clear the filtering database of all entries made from the CLI for a given MAC address, interface or VLAN. Use this command without options to clear any entries made from the CLI.

Compare this usage with [clear mac address-table dynamic](#) command.

**Examples** This example shows how to clear all filtering database entries configured through the CLI.

```
awplus# clear mac address-table static
```

This example shows how to clear all filtering database entries for a specific interface configured through the CLI.

```
awplus# clear mac address-table static interface port1.0.3
```

This example shows how to clear filtering database entries configured through the CLI for the MAC address 0000.5E00.5302.

```
awplus# clear mac address-table static address 0000.5E00.5302
```

**Related commands** [clear mac address-table dynamic](#)  
[mac address-table static](#)  
[show mac address-table](#)

# clear port counter

**Overview** Use this command to clear the packet counters of the port.

**Syntax** `clear port counter [<port>]`

| Parameter | Description              |
|-----------|--------------------------|
| <port>    | The port number or range |

**Mode** Privileged Exec

**Example** To clear the packet counter for port1.0.1, use the command:

```
awplus# clear port counter port1.0.1
```

**Related commands** [show platform port](#)

# debug platform packet

**Overview** This command enables platform to CPU level packet debug functionality on the device.

Use the **no** variant of this command to disable platform to CPU level packet debug. If the result means both send and receive packet debug are disabled, then any active timeout will be canceled.

**Syntax** `debug platform packet [recv] [send] [timeout <timeout>] [vlan 1]`  
`no debug platform packet [recv] [send]`

| Parameter         | Description   |
|-------------------|---|
| recv              | Debug packets received.   |
| send              | Debug packets sent.   |
| timeout <timeout> | Stop debug after a specified time. Specify the time in seconds. |
| vlan 1            | Limit debug to VLAN1.   |

**Default** A 5 minute timeout is configured by default if no other timeout duration is specified.

**Mode** Privileged Exec and Global Configuration

**Usage notes** This command can be used to trace packets sent and received by the CPU. If a timeout is not specified, then a default 5 minute timeout will be applied.

If a timeout of 0 is specified, packet debug will be generated until the **no** variant of this command is used or another timeout value is specified. The timeout value applies to both send and receive debug and is updated whenever the **debug platform packet** command is used.

**Examples** To enable both receive and send packet debug for the default timeout of 5 minutes, enter:

```
awplus# debug platform packet
```

To enable receive packet debug for 10 seconds, enter:

```
awplus# debug platform packet recv timeout 10
```

To enable send packet debug with no timeout, enter:

```
awplus# debug platform packet send timeout 0
```

To enable VLAN packet debug for VLAN 1 with a timeout duration of 3 minutes, enter:

```
awplus# debug platform packet vlan 1 timeout 150
```

To disable receive packet debug, enter:

```
awplus# no debug platform packet recv
```

**Related  
commands**

[show debugging platform packet](#)

[undebug platform packet](#)

# duplex

**Overview** This command changes the duplex mode for the specified port.

To see the currently-negotiated duplex mode for ports whose links are up, use the command [show interface](#). To see the configured duplex mode (when different from the default), use the command [show running-config](#).

**Syntax** duplex {auto|full|half}

| Parameter | Description                       |
|-----------|-----------------------------------|
| auto      | Auto-negotiate duplex mode.       |
| full      | Operate in full duplex mode only. |
| half      | Operate in half duplex mode only. |

**Default** By default, ports auto-negotiate duplex mode (except for 100Base-FX ports which do not support auto-negotiation, so default to full duplex mode).

**Mode** Interface Configuration

**Examples** To specify full duplex for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex full
```

To specify half duplex for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex half
```

To auto-negotiate duplex mode for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex auto
```

**Related commands** [polarity](#)  
[speed](#)  
[show interface](#)

# flowcontrol (switch port)

**Overview** Use this command to enable flow control, and configure the flow control mode for the switch port.

Use the **no** variant of this command to disable flow control for the specified switch port.

**Syntax** `flowcontrol both`  
`flowcontrol {send|receive} {off|on}`  
`no flowcontrol`

| Parameter            | Description  |
|----------------------|--|
| <code>both</code>    | Use this parameter to specify send and receive flow control for the port.  |
| <code>receive</code> | When the port receives pause frames, it temporarily stops (pauses) sending traffic.  |
| <code>on</code>      | Enable the specified flow control.   |
| <code>off</code>     | Disable the specified flow control.  |
| <code>send</code>    | When the port is congested (receiving too much traffic), it sends pause frames to request the other end to temporarily stop (pause) sending traffic. |

**Default** By default, flow control is disabled.

**Mode** Interface Configuration

**Usage notes** The flow control mechanism specified by 802.3x is only for full duplex links. It operates by sending PAUSE frames to the link partner to temporarily suspend transmission on the link.

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion, and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When the local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the congestion period.

For half-duplex links, an older form of flow control known as backpressure is supported. See the related [backpressure](#) command.

For flow control on async serial (console) ports, see the [flowcontrol hardware \(asyn/console\)](#) command.

**Examples** To enable flow control on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol both
```

To disable flow control on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no flowcontrol
```

To enable flow control on port1.0.2 (receive only), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol receive on
```

To enable flow control on port1.0.2 (send only), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol send on
```

To disable flow control on port1.0.2 (receive only), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol receive off
```

To disable flow control on port1.0.2 (send only), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol send off
```

**Related commands** [backpressure](#)  
[show running-config](#)

# linkflap action

**Overview** Use this command to detect flapping on all ports. If more than 15 flaps occur in less than 15 seconds the flapping port will shut down.

Use the **no** variant of this command to disable flapping detection at this rate.

**Syntax** linkflap action [shutdown]  
no linkflap action

| Parameter | Description                       |
|-----------|-----------------------------------|
| linkflap  | Global setting for link flapping. |
| action    | Specify the action for port.      |
| shutdown  | Shutdown the port.                |

**Default** Linkflap action is disabled by default.

**Mode** Global Configuration

**Example** To enable the linkflap action command on the device, use the following commands:

```
awplus# configure terminal  
awplus(config)# linkflap action shutdown
```



# mac address-table acquire

**Overview** Use this command to enable MAC address learning on the device.

Use the **no** variant of this command to disable learning.

**Syntax** mac address-table acquire  
no mac address-table acquire

**Default** Learning is enabled by default for all instances.

**Mode** Global Configuration

**Example** awplus# configure terminal  
awplus(config)# mac address-table acquire

# mac address-table ageing-time

**Overview** Use this command to specify an ageing-out time for a learned MAC address. The learned MAC address will persist for at least the specified time.

The **no** variant of this command will reset the ageing-out time back to the default of 300 seconds (5 minutes).

**Syntax** `mac address-table ageing-time <ageing-timer> none`  
`no mac address-table ageing-time`

| Parameter                         | Description   |
|-----------------------------------|---|
| <code>&lt;ageing-timer&gt;</code> | <code>&lt;10-1000000&gt;</code> The number of seconds of persistence. |
| <code>none</code>                 | Disable learned MAC address timeout.                                  |

**Default** The default ageing time is 300 seconds.

**Mode** Global Configuration

**Examples** The following commands specify various ageing timeouts on the device:

```
awplus# configure terminal
awplus(config)# mac address-table ageing-time 1000
awplus# configure terminal
awplus(config)# mac address-table ageing-time none
awplus# configure terminal
awplus(config)# no mac address-table ageing-time
```

# mac address-table static

**Overview** Use this command to statically configure the MAC address-table to forward or discard frames with a matching destination MAC address.

**Syntax** `mac address-table static <mac-addr> {forward|discard} interface <port> [vlan <vid>]`  
`no mac address-table static <mac-addr> {forward|discard} interface <port> [vlan <vid>]`

| Parameter                           | Description   |
|-------------------------------------|---|
| <code>&lt;mac-addr&gt;</code>       | The destination MAC address in HHHH . HHHH . HHHH format.   |
| <code>interface &lt;port&gt;</code> | Specify a switch port to be cleared from the filtering database. The port can be: <ul style="list-style-type: none"><li>• a switchport (e.g. port1.0.4)</li></ul> |
| <code>vlan 1</code>                 | Apply the command to VLAN1.   |

**Mode** Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# mac address-table static 2222.2222.2222 forward`  
`interface port1.0.2`

**Related commands** [clear mac address-table static](#)  
[show mac address-table](#)

# polarity

**Overview** This command sets the MDI/MDIX polarity on a copper-based switch port.

**Syntax** `polarity {auto|mdi|mdix}`

| Parameter | Description  |
|-----------|--|
| mdi       | Sets the polarity to MDI (medium dependent interface).                       |
| mdix      | Sets the polarity to MDI-X (medium dependent interface crossover).           |
| auto      | The switch port sets the polarity automatically. This is the default option. |

**Default** By default, switch ports set the polarity automatically (**auto**).

**Mode** Interface Configuration

**Usage notes** We recommend the default **auto** setting for MDI/MDIX polarity. Polarity applies to copper 10BASE-T, 100BASE-T, and 1000BASE-T switch ports; it does not apply to fiber ports. See the “MDI/MDIX Connection Modes” section in the [Switching Feature Overview and Configuration Guide](#) for more information.

**Example** To set the polarity for port1.0.4 to fixed MDI mode, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# polarity mdi
```

# show debugging platform packet

**Overview** This command shows platform to CPU level packet debugging information.

**Syntax** show debugging platform packet

**Mode** User Exec and Privileged Exec

**Example** To display the platform packet debugging information, use the command:

```
awplus# show debugging platform packet
```

**Related commands** [debug platform packet](#)  
[undebug platform packet](#)

# show flowcontrol interface

**Overview** Use this command to display flow control information.

**Syntax** `show flowcontrol interface <port>`

| Parameter | Description                                     |
|-----------|---|
| <port>    | Specifies the name of the port to be displayed. |

**Mode** User Exec and Privileged Exec

**Example** To display the flow control for port1.0.3, use the command:

```
awplus# show flowcontrol interface port1.0.3
```

**Output** Figure 11-1: Example output from the **show flowcontrol interface** command for a specific interface

| Port      | Send<br>admin | FlowControl<br>oper | Receive<br>admin | FlowControl<br>oper | RxPause | TxPause |
|-----------|---------------|---------------------|------------------|---------------------|---------|---------|
| port1.0.3 | on            | on                  | on               | on                  | 0       | 0       |

# show interface err-disabled

**Overview** Use this command to show the ports which have been dynamically shut down by protocols running on the device and the protocols responsible for the shutdown.

**Syntax** `show interface [<interface-range> err-disabled]`

| Parameter                            | Description  |
|--------------------------------------|--|
| <code>&lt;interface-range&gt;</code> | Interface range                                    |
| <code>err-disabled</code>            | Brief summary of interfaces shut down by protocols |

**Mode** User Exec and Privileged Exec

**Example** To show which protocols have shut down ports, use the commands:

```
awplus# show interface err-disabled
```

# 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
```

Note that this device has one VLAN, the default VLAN (vlan1).

**Output** Figure 11-2: Example output from the **show interface switchport** command

```
AR1050V#show interface switchport
Interface name      : port1.0.1
Switchport mode    : access
Ingress filter     : enable
Acceptable frame types : all
Default Vlan       : 1
Configured Vlans   : 1
Dynamic Vlans      :

Interface name      : port1.0.2
Switchport mode    : access
Ingress filter     : enable
Acceptable frame types : all
Default Vlan       : 1
Configured Vlans   : 1
Dynamic Vlans      :
...
```

**Related commands** [show interface memory](#)



# show mac address-table

**Overview** Use this command to display the MAC address-table for all configured VLANs.

**Syntax** show mac address-table

**Mode** User Exec and Privileged Exec

**Usage notes** The **show mac address-table** command is only applicable to view a MAC address-table for Layer 2 switched traffic within VLANs.

**Example** To display the mac address-table, use the following command:

```
awplus# show mac address-table
```

**Output** See the following sample output captured when there was no traffic being switched:

```
awplus#show mac address-table

VLAN port          mac                type
1     unknown       0000.cd28.0752    forward  static
ARP  -              0000.cd00.0000    forward  static
```

See the sample output captured when packets were switched and MAC addresses were learned:

```
awplus#show mac address-table

VLAN port          mac                type
1     unknown       0000.cd28.0752    forward  static
1     port1.0.2      0030.846e.9bf4    forward  dynamic
1     port1.0.3      0030.846e.bac7    forward  dynamic
ARP  -              0000.cd00.0000    forward  static
```

Note the new MAC addresses learned for port1.0.2 and port1.0.3 added as dynamic entries.

Also note if manually configured static MAC addresses exist, this is shown to the right of the type column:

```
awplus(config)#mac address-table static 0000.1111.2222 for int
port1.0.3 vlan 1
awplus(config)#end
awplus#
awplus#show mac address-table
```

| VLAN | port      | mac            | type    |         |
|------|-----------|----------------|---------|---------|
| 1    | unknown   | 0000.cd28.0752 | forward | static  |
| 1    | port1.0.2 | 0030.846e.bac7 | forward | dynamic |
| 1    | port1.0.3 | 0000.1111.2222 | forward | static  |
| ...  |           |                |         |         |

- Related commands**
- [clear mac address-table dynamic](#)
  - [clear mac address-table static](#)
  - [mac address-table static](#)

# show platform

**Overview** This command displays the settings configured by using the **platform** commands.

**Syntax** `show platform`

**Mode** Privileged Exec

**Usage notes** This command displays the settings in the running config. For changes in some of these settings to take effect, the device must be rebooted with the new settings in the startup config.

**Example** To check the settings configured with **platform** commands on the device, use the following command:

```
awplus# show platform
```

**Output** Figure 11-3: Example output from the **show platform** command

```
awplus#show platform
MAC vlan hashing algorithm    unknown
```

**Table 1:** Parameters in the output of the **show platform** command. Note that the parameters displayed depend on your device, and that not all displayed parameters can be modified on all devices.

| Parameter                    | Description   |
|------------------------------|---|
| Routing Ratio                | Whether all memory is allocated to IPv4 address table entries only, or whether it is allocated evenly to both IPv4 and IPv6 addresses (set with the <b>platform routingratio</b> command).  |
| Route Weighting              | The split between multicast and unicast route entries (set with the <b>platform routingratio</b> command).  |
| MAC vlan hashing algorithm   | The MAC VLAN hash-key-generating algorithm (set with the <b>platform mac-vlan-hashing-algorithm</b> command). The default algorithm is crc32l. The algorithm may need to be changed in rare circumstances in which hash collisions occur. |
| L3 hashing algorithm         | The L3 VLAN hash-key-generating algorithm (set with the <b>platform l3-vlan-hashing-algorithm</b> command). The default algorithm is crc32l. The algorithm may need to be changed in rare circumstances in which hash collisions occur.   |
| Load Balancing               | Which packet fields are used in the channel load balancing algorithm (set with the <b>platform load-balancing</b> command).   |
| Control-plane-prioritization | Maximum traffic rate on the CPU port (set with the <b>platform control-plane-prioritization rate</b> command).  |

**Table 1:** Parameters in the output of the **show platform** command. Note that the parameters displayed depend on your device, and that not all displayed parameters can be modified on all devices. (cont.)

| Parameter                     | Description   |
|-------------------------------|---|
| Fdb-chain-length              | The length of the FDB hash chain (set with the <b>platform fdb-chain-length</b> command). FDB entries are hashed and indexed using a hash. In rare circumstances it may be useful to reduce the chain length.   |
| L2MC overlapped group check   | Whether Layer 2 multicast entries are checked before deletion (set with the <b>platform l2mc-overlap</b> command).  |
| silicon-profile               | The silicon profile setting (set with the <b>platform silicon-profile</b> command) for the switch hardware; one of: <ul style="list-style-type: none"> <li>• profile 1</li> <li>• profile 2</li> <li>• profile 3</li> <li>• None (default)</li> </ul>   |
| fdb-l3-hosts mode             | Whether Host Mode is turned on or not. Host Mode increases the number of host entries and is available for systems containing SBx81CFC960 controller cards and SBx81XLEM line cards. See <b>platform silicon-profile</b> and <b>platform fdb-l3-hosts</b> for details.  |
| Jumboframe support            | Whether the jumbo frames setting is enabled or disabled (set with the <b>platform jumboframe</b> command).  |
| Traffic Manager               | A test setting that is disabled by default.   |
| stop-unreg-mc-flooding        | Whether the stop-unreg-mc-flooding feature is on or off (set with the <b>platform stop-unreg-mc-flooding</b> command). This feature prevents flooding of unregistered multicast packets in the occasional situations in which IGMP snooping does not prevent it.  |
| Port Mode                     | Whether each port on the AT-StackQS is configured as one 40Gbps port or four 10Gbps ports, if they are operating as network ports (set with the <b>platform portmode interface</b> command).  |
| Vlan-stacking TPID            | The value of the TPID set in the Ethernet type field when a frame has a double VLAN tag (set with the <b>platform vlan-stacking-tpid</b> command).  |
| PBR enabled                   | Whether policy-based routing is globally enabled or not (set with the <b>platform pbr-enable</b> command).  |
| Hardware Filter Size          | Whether hardware ACLs can filter on IPv6 addresses (ipv4-full-ipv6) or not (ipv4-limited-ipv6). This is set with the <b>platform hwfilter-size</b> command.   |
| Vlan Ingress Filter Hard Drop | The Bridge Vlan Ingress Filtering drops traffic if the VID assigned to the packet does not match with the port's VLAN membership. There are two ways the traffic is dropped by the Ingress Filtering mechanism: <ul style="list-style-type: none"> <li>• HARD DROP - Traffic is dropped by the Bridge Engine and not forwarded or trapped.</li> <li>• SOFT DROP - Traffic may be mirrored or trapped by the Bridge Engine.</li> </ul> |

# show platform port

**Overview** This command displays the various port registers or platform counters for specified switchports.

**Syntax** `show platform port [<port-list>] [counters]`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;port-list&gt;</code> | The ports to display information about. A port-list can be: <ul style="list-style-type: none"><li>• a switchport (e.g. port1.0.4)</li><li>• a continuous range of ports separated by a hyphen (e.g. port1.0.1-1.0.4)</li><li>• a comma-separated list (e.g. port1.0.1,port1.0.3-1.0.4).</li></ul> |
| <code>counters</code>          | Show the platform counters.   |

**Mode** Privileged Exec

**Examples** To display port registers for port1.0.1 to port1.0.4, use the command:

```
awplus# show platform port port1.0.1-port1.0.4
```

To display platform counters for port1.0.1 to port1.0.4, use the command:

```
awplus# show platform port port1.0.1-port1.0.4 counters
```

**Output** Figure 11-4: Example output from the **show platform port** command

```
awplus#show platform port
Phy register value for port1.0.1 (ifindex: 5001)

00:1140 01:796d 02:0143 03:bf88 04:01e1 05:c1e1 06:006d 07:2001
08:495f 09:0600 0a:7800 0b:0000 0c:0000 0d:0000 0e:0000 0f:3000
10:0021 11:2f00 12:0000 13:0000 14:0000 15:0001 16:0000 17:0f08
18:7277 19:871c 1a:243e 1b:ffff 1c:38ff 1d:2556 1e:0000 1f:0000
sfp phy

00:1140 01:796d 02:0143 03:bf88 04:01e1 05:c1e1 06:006d 07:2001
08:495f 09:0600 0a:7800 0b:0000 0c:0000 0d:0000 0e:0000 0f:3000
10:0021 11:2f00 12:0000 13:0000 14:0000 15:0001 16:0000 17:0f08
18:7277 19:871c 1a:0000 1b:ffff 1c:38ff 1d:2556 1e:0000 1f:0000

Port configuration for lport 0x08000000:
Phy Driver: ROBO 546X Gigabit PHY Driver
enabled: 1
loopback: 0
link: 1
speed: 1000 max speed: 1000
duplex: 1
linkscan: 1
autonegotiate: 1
master: 2
tx pause: 0 rx pause: 0
untagged vlan: 1
vlan filter: 1
stp state: 4
learn: 5
discard: 0
jam: 0
max frame size: 1500
MC Disable SA: no
MC Disable TTL: no
MC egress untag: 0
MC egress vid: 0
MC TTL threshold: 0
...
```

# show storm-control

**Overview** Use this command to display storm-control information for all interfaces or a particular interface.

**Syntax** `show storm-control [<port>]`

| Parameter                 | Description   |
|---------------------------|---|
| <code>&lt;port&gt;</code> | The port to display information about. The port may be: <ul style="list-style-type: none"><li>a switchport (e.g. port1.0.4)</li></ul> |

**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 11-5: Example output from the **show storm-control** command for port1.0.2

| Port      | BcastLevel | McastLevel | DlfLevel |
|-----------|------------|------------|----------|
| port1.0.2 | 40.0%      | 100.0%     | 100.0%   |

**Related commands** [storm-control level](#)

# speed

**Overview** This command changes the speed of the specified port. You can optionally specify the speed or speeds that get autonegotiated, so autonegotiation is only attempted at the specified speeds.

To see the currently-negotiated speed for ports whose links are up, use the [show interface](#) command. To see the configured speed (when different from the default), use the [show running-config](#) command.

**Syntax** `speed {10|100|1000}`  
`speed auto [10] [100] [1000]`

The following table shows the speed options for each type of port.

| Port type          | Speed Options (units are Mbps)      |
|--------------------|-------------------------------------|
| RJ-45 copper ports | auto (default)<br>10<br>100<br>1000 |

**Mode** Interface Configuration

**Default** By default, ports autonegotiate speed.

**Usage notes** We recommend having autonegotiation enabled for link speeds of 1000 Mbps and above. For example, to apply a fixed speed of 1000 Mbps use the command **speed auto 1000**.

If multiple speeds are specified after the auto option to autonegotiate speeds, then the device only attempts autonegotiation at those specified speeds.

**Examples** To set the speed of a tri-speed port to 100 Mbps, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed 100
```

To return the port to auto-negotiating its speed, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed auto
```

To set the port to auto-negotiate its speed at 100 Mbps and 1000 Mbps, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed auto 100 1000
```



To set the port to auto-negotiate its speed at 1000 Mbps only, which will fix this port speed to 1000 Mbps, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed auto 1000
```

**Related  
commands**

[duplex](#)  
[polarity](#)  
[show interface](#)  
[speed \(asyn\)](#)

# storm-control level

**Overview** Use this command to specify the speed limiting level for broadcast, multicast, or dlf (destination lookup failure) traffic for the port. Storm-control limits the selected traffic type to the specified percentage of the maximum port speed.

Use the **no** variant of this command to disable storm-control for broadcast, multicast or dlf traffic.

**Syntax** `storm-control {broadcast|dlf} level <level>`  
`no storm-control {broadcast|dlf} level`

| Parameter | Description  |
|-----------|--|
| <level>   | <0-100> Specifies the percentage of the maximum port speed allowed for broadcast, multicast or destination lookup failure traffic. |
| broadcast | Applies the storm-control to broadcast frames.   |
| dlf       | Applies the storm-control to destination lookup failure traffic.   |

**Default** Disabled

**Mode** Interface Configuration

**Usage notes** Flooding techniques are used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

More than one limit type can be set at a time. For example, you can configure both broadcast and multicast levels on the same port, at the same time.

**Example** To limit broadcast traffic on port1.0.2 to 30% of the maximum port speed, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# storm-control broadcast level 30
```

**Related commands** [show storm-control](#)

**Command changes** Version 5.4.9-1.3: Multiple limit types available on x530 series

# undebbug platform packet

**Overview** This command applies the functionality of the no `debug platform packet` command.

# 12

# Bridging Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure bridging. For more information, see the [Bridging Feature Overview and Configuration Guide](#).

- Command List**
- “ageing-time” on page 398
  - “bridge” on page 399
  - “bridge-group” on page 400
  - “clear mac-filter counter” on page 401
  - “default-action” on page 402
  - “default-protocol-action” on page 404
  - “l3-filtering enable” on page 405
  - “mac-filter-group egress” on page 406
  - “mac-filter” on page 407
  - “mac-filter-group” on page 408
  - “mac-learning” on page 409
  - “protocol ethii (macfilter)” on page 410
  - “protocol novell (macfilter)” on page 412
  - “protocol sap (macfilter)” on page 414
  - “protocol snap (macfilter)” on page 416
  - “rule (macfilter)” on page 418
  - “rule ip (macfilter)” on page 420
  - “rule ipv6 (macfilter)” on page 422
  - “show bridge” on page 424

- [“show bridge macaddr”](#) on page 426
- [“show mac-filter”](#) on page 427

# ageing-time

**Overview** This command specifies the time period that a learned MAC address will remain defined within the bridge's MAC address table.

Use the **no** variant of this command to set the ageing out time back to the default.

**Syntax** ageing-time <10-1000000>  
no ageing-time

| Parameter    | Description  |
|--------------|--|
| <10-1000000> | The number of seconds that the MAC addresses will remain in the table. |

**Default** 300 seconds (5 minutes)

**Mode** Interface Configuration

**Examples** To change the ageing time on br2 to 60 seconds (1 minute), use the following commands:

```
awplus#configure terminal
awplus(config)#interface br2
awplus(config-if)#ageing-time 60
```

To reset the ageing time back to its default, use the following commands:

```
awplus#configure terminal
awplus(config-if)#no ageing-time
```

To reset the ageing time back to its default, you can also use the following commands:

```
awplus#configure terminal
awplus(config-if)#ageing-time 300
```

**Output** None

**Related commands** [bridge](#)  
[bridge-group](#)  
[show bridge](#)  
[show bridge macaddr](#)

# bridge

**Overview** Use this command to create a software bridge.

Use the **no** variant of this command to remove the specified bridge.

**Syntax** `bridge <bridge-id>`  
`no bridge <bridge-id>`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;bridge-id&gt;</code> | The bridge ID (from 1 to 64). This is made up of the bridge priority and the bridge's MAC address. |

**Default** No configured bridges

**Mode** Global Configuration

**Usage notes** The bridge interface name will be prefixed with 'br' followed by the bridge ID.  
*If interfaces exist on a bridge, then the bridge cannot be removed. For example if interface eth1 exists on bridge 2, then the **no bridge 2** command will give you the following message:*

```
% failed to remove interface br2, there are still configured sub-interfaces.
```

**Example** To create a bridge with the ID of 2, use the following commands:

```
awplus#configure terminal  
awplus(config)#bridge 2
```

To remove the bridge with the ID of 2, use the following commands:

```
awplus#configure terminal  
awplus(config)##no bridge 2
```

**Related commands**

- [ageing-time](#)
- [bridge-group](#)
- [show bridge](#)
- [show bridge macaddr](#)

# bridge-group

**Overview** Use this command to add an interface to a bridge. Interfaces that have been added to a bridge will lose their L3 properties.

Use the **no** variant of this command to remove an interface from a bridge.

**Syntax** `bridge-group <0-255>`  
`no bridge-group`

| Parameter | Description   |
|-----------|---|
| <0-255>   | The ID of the bridge that you are adding the interface to. Interface ID 0 is a VLAN-aware bridge. For more information about the VLAN-aware bridge, see the <a href="#">Bridging Feature Overview and Configuration Guide</a> . |

**Default** An interface is not part of any bridge by default

**Mode** Interface Configuration

**Usage notes** Interfaces can only be part of one bridge, so when removing the bridge no parameters are required.

Interfaces that have been added to a bridge will lose their Layer 3 properties. The bridge will act as the Layer 3 interface. The bridge will provide Layer 2 connectivity between interfaces that are a part of the same bridge-group.

You can attached interfaces such as Ethernet, VLAN, VTI (Tunnel) to your bridge.

**Examples** To add eth1 to bridge 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# bridge-group 2
```

To remove eth1 from your bridge, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no bridge-group
```

**Related commands**

- [ageing-time](#)
- [bridge](#)
- [show bridge](#)
- [show bridge macaddr](#)



# clear mac-filter counter

**Overview** This command clears all the mac-filter counters on a bridge interface.

**Syntax**

```
clear mac-filter counter  
clear mac-filter counter ingress  
clear mac-filter counter egress  
clear mac-filter counter {ingress|egress} <interface-name>
```

| Parameter        | Description                               |
|------------------|---|
| ingress          | Clear only the ingress counters           |
| egress           | Clear only the egress counters            |
| <interface-name> | Clear counters on the specified interface |

**Default** None

**Mode** Privileged Exec

**Examples** To clear all ingress counters on eth1, use the following command:

```
awplus#clear mac-filter counter ingress eth1
```

To clear all ingress counters, use the following command:

```
awplus#clear mac-filter counter ingress
```

To clear all mac-filter counters, use the following command:

```
awplus#clear mac-filter counter
```

**Related commands**

- [mac-filter](#)
- [mac-filter-group](#)
- [show mac-filter](#)
- [rule \(macfilter\)](#)

**Command changes** Version 5.4.8-0.2: command updated

# default-action

**Overview** Use this command to set the default action for packets not hitting a particular mac-filter.

Use the **no** variant of this command to remove the configured default action. See the third example below for more information.

**Syntax** `default-action [permit|deny|none]`  
`no default-action`

| Parameter | Description   |
|-----------|---|
| permit    | Accept the traffic which didn't match any rule in the mac-filter. This means the traffic will not pass through any other mac-filters. |
| deny      | Drop the traffic which didn't hit any rule in the mac-filter.   |
| none      | Allow the traffic (which didn't hit any rule in the mac-filter) to traverse the next mac-filter, if any are configured.               |

**Default** Deny.

**Mode** MAC Filter Configuration

**Example 1** To set the default action to **none** for the mac-filter named: filter1, use the following commands:

```
awplus# configure terminal
awplus(config)# mac-filter filter1
awplus(config-macfilter)# default-action none
```

This means that if this filter is set on ingress traffic for eth1 and that traffic doesn't hit any rules in the filter, then the traffic will progress to any other filters present. For example, there could be a filter on bridge1 that eth1 is a part of. If bridge1 also has mac filters, then those filters have a chance to examine that traffic ingressing eth1.

**Example 2** To set the default action to **permit** for the mac-filter named: filter1, use the following commands:

```
awplus# configure terminal
awplus(config)# mac-filter filter1
awplus(config-macfilter)# default-action permit
```

This means that if this filter is set on ingress traffic for eth1 and that traffic doesn't hit any rules in the filter, then the traffic will not progress to any other filters present, and will not undergo any more filtering.

**Example 3** To set the default action to **deny** for the mac-filter named: filter1, use the following commands:

```
awplus# configure terminal
awplus(config)# mac-filter filter1
awplus(config-macfilter)# default-action deny
```

This means that if this filter is set on ingress traffic for eth1 and that traffic doesn't hit any rules in the filter, then the traffic will be dropped. This is the same as setting the command **no default-action**.

**Related commands** [mac-filter](#)

**Command changes** Version 5.4.7-2.1: command added

# default-protocol-action

**Overview** Use this command to set the default behavior (permit or deny) when a packet does not match any configured protocol filter. Permit means to continue to the rules (if rules exist). If there are no rules or no rules match, then continue to the default action.

Use the **no** variant of this command to revert to the default filtering action of 'permit'.

**Syntax** `default-protocol-action {permit|deny}`  
`no default-protocol-action`

| Parameter | Description      |
|-----------|------------------|
| permit    | Allow the packet |
| deny      | Drop the packet  |

**Default** Permit.

**Mode** MAC Filter Configuration

**Example** To designate ATL-router1 to deny all packets that do not match the configured protocol filters, use the following commands:

```
awplus# configure terminal
awplus(config)# mac-filter ATL-router1
awplus(config-macfilter)# default-protocol-action deny
```

**Related commands** [protocol ethii \(macfilter\)](#)  
[protocol novell \(macfilter\)](#)  
[protocol sap \(macfilter\)](#)  
[protocol snap \(macfilter\)](#)

**Command changes** Version 5.4.8-0.2: command added

# I3-filtering enable

**Overview** Use this command to enable traffic control for bridged traffic on a bridge interface.

Use the **no** variant of this command to disable traffic control for bridged traffic on a bridge interface.

**Syntax** l3-filtering enable  
no l3-filtering enable

**Default** Traffic control is disabled by default for bridged traffic.

**Mode** Interface mode for a bridge interface

**Example** To enable traffic control for bridged traffic on br1, use the commands:

```
awplus# configure terminal
awplus(config)# interface br1
awplus(config-if)# l3-filtering enable
```

**Command changes** Version 5.4.7-0.1: command added. Previously, traffic control was enabled by default on all bridge interfaces.

# mac-filter-group egress

**Overview** Use this command to apply an egress MAC-filter to a bridge interface, bridge port, or potential bridge port.

Use the **no** variant of this command to remove an egress MAC-filter on a specific bridge interface or bridge port.

**Syntax** `mac-filter-group egress <mac-filter-name>`  
`no mac-filter-group egress`

| Parameter                            | Description  |
|--------------------------------------|--|
| <code>&lt;mac-filter-name&gt;</code> | The name of the MAC-filter that is applied to the bridge interface or bridge port on egress. |

**Default** No mac-filter.

**Mode** Interface Configuration

**Example** To configure MAC-filter 'filter1' to operate on traffic egressing tunnel2, use the following commands:

```
awplus# configure terminal
awplus(config)# int tunnel2
awplus(config-if)# mac-filter-group egress filter1
```

To remove that same filter, use the following commands:

```
awplus# configure terminal
awplus(config)# int tunnel2
awplus(config-if)# no mac-filter-group egress
```

**Related commands** [mac-filter](#)  
[show mac-filter](#)  
[clear mac-filter counter](#)

**Command changes** Version 5.4.8-0.2 command updated.

# mac-filter

**Overview** This command creates a Layer 2 MAC filter that can be applied on a bridge. Use the **no** variant of this command to remove the MAC filter.

**Syntax** `mac-filter [<mac-filter-name>]`  
`no mac-filter [<mac-filter-name>]`

| Parameter                      | Description  |
|--------------------------------|--|
| <i>&lt;mac-filter-name&gt;</i> | The name of the mac-filter (maximum of 16 characters). |

**Default** None

**Mode** Interface Configuration

**Usage notes** You can only create one MAC filter at one time.

**Examples** To create a mac-filter with the name of ATL-router1, use the following commands:

```
awplus#configure terminal  
awplus(config)#mac-filter ATL-router1
```

To delete a mac-filter, use the following commands:

```
awplus#configure terminal  
awplus(config)#no mac-filter ATL-router1
```

**Output** None

**Related commands** [clear mac-filter counter](#)  
[mac-filter-group](#)  
[show mac-filter](#)

# mac-filter-group

**Overview** This command applies a Layer two MAC filter on a bridge.  
Use the **no** variant of this command to remove the mac-filter on a bridge.

**Syntax** `mac-filter-group [<mac-filter-name>]`  
`no mac-filter-group`

| Parameter                      | Description   |
|--------------------------------|---|
| <i>&lt;mac-filter-name&gt;</i> | The name of the mac-filter (maximum 16 characters). |

**Default** None

**Mode** Interface Configuration

**Usage notes** You can only apply one MAC filter at one time.

**Examples** To apply a mac-filter with the name of ATL-router1 on bridge interface br1, use the following commands:

```
awplus#configure terminal
awplus(config)#interface br1
awplus(config-if)#mac-filter-group ATL-router1
```

To remove the mac-filter on a bridge, use the following commands:

```
awplus#configure terminal
awplus(config)#interface br1
awplus(config-if)#no mac-filter-group
```

**Output** Figure 12-1: Example output from the **mac-filter-group** command displaying information about all bridges:

```
mac-filter "ATL-router1" will be applied to the bridge interface
br1
```

**Related commands**

- [clear mac-filter counter](#)
- [mac-filter](#)
- [show mac-filter](#)



# mac-learning

**Overview** Use this command to enable FDB MAC address learning on a bridge interface. In some circumstances, FDB MAC address learning on a software-based router bridge is not useful, and it is better to flood the traffic within interfaces associated with the bridge instance, to ensure the traffic reaches its destination.

Use the **no** variant of this command to disable or enable FDB MAC address learning on a bridge.

**Syntax** `mac-learning`  
`no mac-learning`

**Default** Learning is enabled by default.

**Mode** Interface mode for a bridge interface

**Example** To turn off learning on bridge 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface br2
awplus(config-if)# no mac-learning
```

To turn learning on bridge 2 back on, use the following commands:

```
awplus# configure terminal
awplus(config)# interface br2
awplus(config-if)# mac-learning
```

**Command changes** Version 5.4.7-0.1: command added

# protocol ethii (macfilter)

**Overview** Use this command to add a bridge protocol filter for Ethernet II packets. If ether-type is not specified, then all Ethernet II packets match the rule.

If ether-type is specified, then only packets having the specified ether-type matches the rule.

Use the **no** variant of this command to remove the protocol filter.

**Syntax**

```
protocol <filter-name> {permit|deny} ethii
protocol <filter-name> {permit|deny} ethii ether-type
<ether-type>
protocol <filter-name> {permit|deny} ethii {after|before}
protocol <filter-name>
protocol <filter-name> {permit|deny} ethii ether-type
<ether-type> {after|before} protocol <filter-name>
no protocol <filter-name>
```

| Parameter     | Description  |
|---------------|--|
| <filter-name> | Protocol filter name.  |
| permit        | Allow the matched frame  |
| deny          | Drop the matched frame   |
| ethii         | Ethernet type II frame   |
| ether-type    | Ethertype of Ethernet II frame   |
| <ether-type>  | Ethertype (2 bytes in hexadecimal, e.g. 0800) or any of the well-known names.. |
| arp           | ARP (Address Resolution Protocol), 0806  |
| atmf          | ATMF (Allied Telesis Management Framework), fbae                               |
| atmf-agent    | ATMF Agent, fbae   |
| ip            | IPv4 (Internet Protocol version 4), 0800                                       |
| ipv6          | IPv6 (Internet Protocol version 6), 86dd                                       |
| loop          | Loopback (Ethernet Configuration Testing Protocol), 9000                       |
| ppp           | PPP (Point-to-Point Protocol), 880b  |
| pppoe-disc    | PPPoE Discovery, 8863  |
| pppoe-sess    | PPPoE Session, 8864  |
| after         | Add after the following protocol filter name                                   |
| before        | Add before the following protocol filter name.                                 |

**Default** The default action is permit.

**Mode** MAC Filter Configuration

**Usage notes** This command adds or deletes a protocol filter for bridged traffic in Mac filter mode.

By default all protocols are permitted, but this can be changed by using the command: **default-protocol-action**.

This command, examines packets for each protocol filter in the configured order.

- If a denied protocol filter is matched, then the packet is immediately dropped without examining the rest of protocol filters and rules
- If a permitted protocol filter is matched, then the packet skips the rest of protocol filters and continues to examine rules.

**Example** To allow all IPv4 packets, use the commands:

```
awplus# configure terminal
awplus(config)# mac-filter ATL-router1
awplus(config-macfilter)# protocol 1 permit ethii ether-type ip
```

**Related commands**

- [rule \(macfilter\)](#)
- [rule ip \(macfilter\)](#)
- [rule ipv6 \(macfilter\)](#)
- [default-protocol-action](#)
- [show mac-filter](#)
- [clear mac-filter counter](#)

**Command changes** Version 5.4.8-0.2: command added

# protocol novell (macfilter)

**Overview** Use this command to add a bridge protocol filter for Novell raw IEEE 802.3 packets..  
Use the **no** variant of this command to remove the protocol filter.

**Syntax**

```
protocol <filter-name> {permit|deny} novell  
protocol <filter-name> {permit|deny} novell {after|before}  
protocol <filter-name>  
  
no protocol <filter-name>
```

| Parameter     | Description                                    |
|---------------|--|
| <filter-name> | Protocol filter name.                          |
| permit        | Allow the matched frame                        |
| deny          | Drop the matched frame                         |
| novell        | Novell raw IEEE 802.3                          |
| after         | Add after the following protocol filter name   |
| before        | Add before the following protocol filter name. |

**Default** The default action is permit.

**Mode** MAC Filter Configuration

**Usage notes** This command adds or deletes a protocol filter for bridged traffic in Mac filter mode.

By default all protocols are permitted, but this can be changed by using the command: **default-protocol-action**.

This command, examines packets for each protocol filter in the configured order.

- If a denied protocol filter is matched, then the packet is immediately dropped without examining the rest of protocol filters and rules
- If a permitted protocol filter is matched, then the packet skips the rest of protocol filters and continues to examine rules.

**Example** To allow all Novell IEEE 802.3 packets, use the commands:

```
awplus# configure terminal  
awplus(config)# mac-filter ATL-router1  
awplus(config-macfilter)# protcol 1 permit novell
```

**Related commands**

- [rule \(macfilter\)](#)
- [rule ip \(macfilter\)](#)
- [rule ipv6 \(macfilter\)](#)

default-protocol-action

show mac-filter

clear mac-filter counter

**Command changes** Version 5.4.8-0.2: command added

# protocol sap (macfilter)

**Overview** Use this command to add a bridge protocol filter for IEEE 802.3 packets. If `sap-type` is not specified, then all IEEE 802.3 packets (including Novell raw IEEE 802.3, IEEE 802.3 with 802.2 LLC and IEEE 802.3 with 802.2 SNAP) match the rule.

If `sap-type` is specified, then only packets having the specified `sap-type` matches the rule.

Use the **no** variant of this command to remove the protocol filter.

**Syntax**

```
protocol <filter-name> {permit|deny} sap
protocol <filter-name> {permit|deny} sap sap-type <sap-type>
protocol <filter-name> {permit|deny} sap {after|before}
protocol <filter-name>
protocol <filter-name> {permit|deny} sap sap-type <sap-type>
{after|before} protocol <filter-name>
no protocol <filter-name>
```

| Parameter     | Description                                     |
|---------------|---|
| <filter-name> | Protocol filter name.                           |
| permit        | Allow the matched frame                         |
| deny          | Drop the matched frame                          |
| sap           | SAP (IEEE 802.3)                                |
| sap-type      | SAP type  |
| <sap-type>    | SAP type value (1 byte in hexadecimal, e.g. e0) |
| after         | Add after the following protocol filter name    |
| before        | Add before the following protocol filter name.  |

**Default** The default action is permit. You can change the default by using the command: **default-protocol-action**.

**Mode** MAC Filter Configuration

**Usage notes** This command adds or deletes a protocol filter for bridged traffic in Mac filter mode.

This command, examines packets for each protocol filter in the configured order.

- If a denied protocol filter is matched, then the packet is immediately dropped without examining the rest of protocol filters and rules
- If a permitted protocol filter is matched, then the packet skips the rest of protocol filters and continues to examine rules.

**Example** To allow Novell Netware SAP type of 802.2 packets, use the commands:

```
awplus# configure terminal
awplus(config)# mac-filter ATL-router1
awplus(config-macfilter)# protocol 2 permit sap sap-type e0
```

**Related  
commands**

rule (macfilter)  
rule ip (macfilter)  
rule ipv6 (macfilter)  
default-protocol-action  
show mac-filter  
clear mac-filter counter

**Command  
changes**

Version 5.4.8-0.2: command added

# protocol snap (macfilter)

**Overview** Use this command to add a bridge protocol filter for SNAP (IEEE 802.3 with 802.2 SNAP) packets. If snap-type is not specified, then all snap packets match the rule.

If snap-type is specified, then only packets having the specified snap-type matches the rule.

Use the **no** variant of this command to remove the protocol filter.

**Syntax**

```
protocol <filter-name> {permit|deny} snap
protocol <filter-name> {permit|deny} snap-type <snap-type>
protocol <filter-name> {permit|deny} snap {after|before}
protocol <filter-name>
protocol <filter-name> {permit|deny} snap snap-type <snap-type>
{after|before} protocol <filter-name>
no protocol <filter-name>
```

| Parameter     | Description  |
|---------------|--|
| <filter-name> | Protocol filter name.                                |
| permit        | Allow the matched frame                              |
| deny          | Drop the matched frame                               |
| snap          | IEEE 802.2 SNAP                                      |
| snap-type     | SNAP type  |
| <snap-type>   | SNAP protocol ID (2 bytes in hexadecimal, e.g. 0800) |
| after         | Add after the following protocol filter name         |
| before        | Add before the following protocol filter name.       |

**Default** The default action is permit.

**Mode** MAC Filter Configuration

**Usage notes** This command adds or deletes a protocol filter for bridged traffic in Mac filter mode.

By default all protocols are permitted, but this can be changed by using the command: **default-protocol-action**.

This command, examines packets for each protocol filter in the configured order.

- If a denied protocol filter is matched, then the packet is immediately dropped without examining the rest of protocol filters and rules
- If a permitted protocol filter is matched, then the packet skips the rest of protocol filters and continues to examine rules.



**Example** To allow all SNAP packets, use the commands:

```
awplus# configure terminal
awplus(config)# mac-filter ATL-router1
awplus(config-macfilter)# protocol 3 permit snap
```

**Related commands**

- rule (macfilter)
- rule ip (macfilter)
- rule ipv6 (macfilter)
- default-protocol-action
- show mac-filter
- clear mac-filter counter

**Command changes** Version 5.4.8-0.2: command added

# rule (macfilter)

**Overview** Use this command to add a filter rule to a specified mac-filter. The filter rule can also be configured to run after or before the specified rule.

Use the **no** variant of this command to remove a filter rule.

**Syntax** `rule <rule-name> {deny|permit} [dmac {<mac-addr>|any}] [smac {<mac-addr>|any}] [proto {<ether-type>|any}] [offset <0-1499> hex-string <match-string>] [{after|before} rule <rule-name>]`  
`no rule <rule-name>`

| Parameter        | Description  |
|------------------|--|
| <rule-name>      | The name of the rule (maximum of 16 characters)        |
| deny             | Drop the matched frame                                 |
| permit           | Allow the matched frame                                |
| dmac             | Destination MAC address                                |
| smac             | Source MAC address                                     |
| <mac-addr>       | MAC address in HHHH.HHHH.HHHH format                   |
| <ether-type>     | Ethernet protocol type                                 |
| offset           | Offset of Ethernet data to match                       |
| <0-1499>         | Offset value (0 is the beginning of the Ethernet data) |
| hex-string       | Match with the specified hexadecimal string            |
| <match-string>   | String to match in hexadecimal (e.g. 01ab)             |
| after            | Add after the following rule name                      |
| before           | Add before the following rule name                     |
| rule <rule-name> | Mac Filter rule  |

**Mode** MAC Filter Configuration

**Usage notes** The filter rule can specify any combination of the following:

- destination MAC address
- source MAC address
- Ethernet protocol type
- string match from a specific offset of Ethernet data

**Example** To configure a bridge filter rule (RULE1) that permits any destination MAC address with the source address of 00c4.6d20.c0f4 with any protocol, use the following commands:

```
awplus# configure terminal
awplus(config)# mac-filter ATL-router1
awplus(config-macfilter)# rule RULE1 permit dmac any smac
00c4.6d20.c0f4 proto any
```

**Example** To configure a bridge filter rule (RULE2) that permits any broadcast traffic with 0xF2 at the offset of 28 (29th byte) in the Ethernet data, use the following commands:

```
awplus# configure terminal
awplus(config)# mac-filter ATL-router1
awplus(config-macfilter)# rule RULE2 permit dmac ffff.ffff.ffff
offset 28 hex-string f2
```

**Related commands**

- [show mac-filter](#)
- [clear mac-filter counter](#)
- [rule ip \(macfilter\)](#)
- [rule ipv6 \(macfilter\)](#)

**Command changes** Version 5.4.8-0.2: command added

# rule ip (macfilter)

**Overview** Use this command to add a bridge filter rule based on the IP protocol.

Use the **no** variant of this command to remove a bridge IP protocol filter.

**Syntax**

```
rule <name> {deny|permit} ip [src {<ip-addr>|<ip-subnet>}]  
[dst {<ip-addr>|<ip-subnet>}] [proto <1-255>] [{after|before}  
rule <name>]  
  
rule <name> {deny|permit} ip [src {<ip-addr>|<ip-subnet>}]  
[dst {<ip-addr>|<ip-subnet>}] [proto {tcp|udp} [sport  
<1-65535>] [dport <1-65535>]] [{after|before} rule <name>]  
  
no rule <name>
```

| Parameter       | Description                                      |
|-----------------|--|
| <name>          | Rule name  |
| deny            | Drop the matched frame                           |
| permit          | Permit the matched frame                         |
| src <ip-addr>   | Source IP address                                |
| src <ip-subnet> | Source IP address with subnet prefix length      |
| dst <ip-addr>   | Destination IP address                           |
| dst <ip-subnet> | Destination IP address with subnet prefix length |
| proto <1-255>   | IP protocol number                               |
| proto tcp       | TCP protocol                                     |
| proto udp       | UDP protocol                                     |
| sport <1-65535> | TCP or UDP source port number                    |
| dport <1-65535> | TCP or UDP destination port number               |
| after           | Add after the following rule name                |
| before          | Add before the following rule name               |
| rule <name>     | MAC Filter rule name                             |

**Mode** MAC Filter Configuration

**Example** To add a bridge filter rule that permits IP packets with a source address of 192.168.1.1 and a destination address of 10.0.0.0/8 using the TCP protocol to destination port 23, use the following commands:

```
awplus# configure terminal  
awplus(config)# mac-filter ATL-router1  
awplus(config-macfilter)# rule 1 permit ip scr 192.168.1.1 dst  
10.0.0.0/8 proto tcp dport 23
```

**Related commands** show mac-filter  
rule (macfilter)  
default-protocol-action

**Command changes** Version 5.4.8-0.2: command added

# rule ipv6 (macfilter)

**Overview** Use this command to add a bridge filter rule based on the IPv6 protocol.  
Use the **no** variant of this command to remove a bridge IPv6 protocol filter.

**Syntax**

```
rule <name> {deny|permit} ipv6 [src
{<ipv6-addr>|<ipv6-addr/prefix-length>}]
[dst {<ipv6-addr>|<ipv6-addr/prefix-length>}] [proto <1-255>]
[ {after|before} rule <name>]

rule <name> {deny|permit} ipv6 [src
{<ipv6-addr>|<ipv6-addr/prefix-length>}]
[dst {<ipv6-addr>|<ipv6-addr/prefix-length>}] [proto {tcp|udp}
[sport <1-65535>] [dport <1-65535>]] [ {after|before} rule
<name>]

no rule <name>
```

| Parameter                        | Description  |
|----------------------------------|--|
| <name>                           | Rule name  |
| deny                             | Drop the matched frame                             |
| permit                           | Permit the matched frame                           |
| src <ipv6-addr>                  | Source IPv6 address                                |
| src<br><ipv6-addr/prefix-length> | Source IPv6 address with subnet prefix length      |
| dst <ipv6-addr>                  | Destination IPv6 address                           |
| dst<br><ipv6-addr/prefix-length> | Destination IPv6 address with subnet prefix length |
| proto <1-255>                    | IPv6 protocol number                               |
| proto tcp                        | TCP protocol                                       |
| proto udp                        | UDP protocol                                       |
| sport <1-65535>                  | TCP or UDP source port number                      |
| dport <1-65535>                  | TCP or UDP destination port number                 |
| after                            | Add after the following rule name                  |
| before                           | Add before the following rule name                 |
| rule <name>                      | MAC Filter rule name                               |

**Mode** MAC Filter Configuration

**Example** To add a bridge filter rule that permits IPv6 packets with a source address of 2001::1 and a destination address of 3001::/64 using the TCP protocol to destination port 23, use the following commands:

```
awplus# configure terminal
awplus(config)# mac-filter ATL-router1
awplus(config-macfilter)# rule 1 permit ipv6 scr 2001::1 dst
3001::/64 proto tcp dport 23
```

**Related commands** [show mac-filter](#)  
[rule \(macfilter\)](#)  
[protocol sap \(macfilter\)](#)

**Command changes** Version 5.4.8-0.2: command added

# show bridge

**Syntax** Use this command to display detailed information about your bridge(s).

**Syntax** `show bridge [<bridge-list>]`

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;bridge-list&gt;</code> | The bridge/s to display the information about.<br>The <code>&lt;bridge-list&gt;</code> can be: <ul style="list-style-type: none"><li>• a single bridge (e.g. br2)</li><li>• a continuous range of bridges (e.g. br1-3)</li><li>• a comma separated list of bridges and/or ranges (e.g. br1,br2,br3-br5)</li></ul> |

**Default** Displays detailed information about all bridges, if no `<bridge-list>` is specified.

**Mode** Privileged Exec

**Examples** To display information about all bridges, use the following command:

```
awplus#show bridge
```

To display information about bridge 2, use the following command:

```
awplus#show bridge br2
```

To display information about bridge in the range 1 to 3, use the following command:

```
awplus#show bridge br1-3
```

To display information about bridges 1, and from 3 to 5, use the following command:

```
awplus#show bridge br1,br3-5
```

**Output** Figure 12-2: Example output from the **show bridge** command displaying information about all bridges:

```
awplus#show bridge
```

| Bridge Name | Aging Timer | Interfaces |
|-------------|-------------|------------|
| br1         | 300         | eth1       |
| br3         | 300         |            |
| br4         | 300         |            |
| br5         | 300         |            |



Figure 12-3: Example output from the **show bridge** command displaying information about bridge 1.

```
awplus#show bridge br1
Bridge Name      Aging Timer      Interfaces
-----
br1              300              eth1
```

**Related  
commands**

- [ageing-time](#)
- [bridge](#)
- [bridge-group](#)
- [show bridge macaddr](#)

# show bridge macaddr

**Overview** Use this command to display the MAC entries learned in the MAC table for your bridge.

**Syntax** `show bridge macaddr <bridge-list>`

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;bridge-list&gt;</code> | The bridge interfaces to display the information about. The <code>&lt;bridge-list&gt;</code> can be: <ul style="list-style-type: none"><li>• a single bridge (e.g. br2)</li><li>• a continuous range of bridges (e.g. br1-3)</li><li>• a comma separated list of bridges and/or ranges (e.g. br1,br2,br3-br5)</li></ul> |

**Mode** Global Configuration

**Example** To display the learned MAC entries for bridge 2, use the following commands:

```
awplus#configure terminal  
awplus(config)#show bridge macaddr br2
```

**Output** Figure 12-4: Example output from the **show bridge macaddr** command displaying information about bridge 2:

```
awplus#show bridge macaddr br2
```

| Bridge Name | Interface | mac addr          | is local? | ageing |
|-------------|-----------|-------------------|-----------|--------|
| br2         | vlan1     | ec:cd:6d:20:c0:fb | no        | 41     |
| br2         | vlan1     | 00:c4:6d:20:c0:e6 | no        | 0      |
| br2         | vlan1     | ec:cd:6d:20:c0:bd | yes       | 0      |
| ...         |           |                   |           |        |

**Related commands**

- [ageing-time](#)
- [bridge](#)
- [bridge-group](#)
- [show bridge](#)

# show mac-filter

**Overview** This command displays configured protocol filters and rules along with packet and byte counts on a bridge or an interface that is a member of a bridge.

**Syntax** `show mac-filter [<interface-name>]`

| Parameter        | Description  |
|------------------|--|
| <interface-name> | The interface name. Mac-filters applied to this interface will be displayed. |

**Default** Displays all MAC filters, rules, and counters for all interfaces on a bridge.

**Mode** Privileged Exec

**Examples** To display all MAC filters, rules, and counters for all interfaces on a bridge, use the following command:

```
awplus#show mac-filter
```

**Output** Figure 12-5: Example output from **show mac-filter**

```
awplus#show mac-filter
```

| Iface | Rule         | Options                   | Pkt Count  |
|-------|--------------|---------------------------|------------|
|       | Dir / Action |                           | Byte Count |
| br1   | a            | Protocol : Ethernet II    | 0          |
|       | in / deny    | Ether-type : ip           | 0          |
| br1   |              | Protocol (default action) | 0          |
|       | in / permit  |                           | 0          |
| br1   |              | Rule (default action)     | 0          |
|       | in / permit  |                           | 0          |
| vlan1 | 1            | IPv4 Src : any            | 0          |
|       | out / deny   | Dst : 192.168.1.20        | 0          |
|       |              | Proto: any                |            |
| vlan1 | 2            | IPv6 Src : any            | 0          |
|       | out / deny   | Dst : 2001::20            | 0          |
|       |              | Proto: any                |            |
| vlan1 | 20           | DMAC : any                | 0          |
|       | out / permit | SMAC : any                | 0          |
|       |              | Proto : 0x0800            |            |
| vlan1 | 30           | DMAC : any                |            |
|       | out / permit | SMAC : any                | 0          |
|       |              | Proto : any               | 0          |
|       |              | Offset: 10                |            |
|       |              | String: 010203abcd        |            |
| vlan1 |              | Rule (default action)     | 0          |
|       | out / deny   |                           | 0          |

**Related commands** [mac-filter](#)

## mac-filter-group

**Command changes** Version 5.4.8-0.2: command updated

# 13

# PPP Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure and validate the PPP (Point-To-Point) protocol. For more information about PPP, see the [Point-to-Point Protocol \(PPP\) Feature Overview and Configuration Guide](#).

- Command List**
- [“debug ppp”](#) on page 431
  - [“encapsulation ppp”](#) on page 434
  - [“interface \(PPP\)”](#) on page 435
  - [“ip address negotiated”](#) on page 436
  - [“ip tcp adjust-mss”](#) on page 438
  - [“ip unnumbered”](#) on page 440
  - [“ipv6 tcp adjust-mss”](#) on page 442
  - [“keepalive \(PPP\)”](#) on page 444
  - [“mtu \(PPP\)”](#) on page 446
  - [“peer default ip address”](#) on page 447
  - [“peer neighbor-route”](#) on page 449
  - [“ppp authentication”](#) on page 451
  - [“ppp authentication refuse”](#) on page 453
  - [“ppp hostname”](#) on page 455
  - [“ppp ipcp dns”](#) on page 457
  - [“ppp ipcp dns suffix-list”](#) on page 459
  - [“ppp ipcp ip-override”](#) on page 461
  - [“ppp password”](#) on page 462
  - [“ppp service-name \(PPPoE\)”](#) on page 463

- [“ppp timeout idle”](#) on page 464
- [“ppp username”](#) on page 465
- [“show debugging ppp”](#) on page 466
- [“show interface \(PPP\)”](#) on page 467
- [“undebug ppp”](#) on page 471

# debug ppp

**Overview** Use this command to enable PPP protocol debugging on an optionally specified PPP interface or range of PPP interfaces to analyze PPP behavior when diagnosing PPP connectivity issues. If no interface is specified then debugging for all PPP interfaces is enabled.

Use the **no** variant of this command to disable PPP protocol debugging on the specified PPP interface. If no PPP interface is specified then PPP debugging for all PPP interfaces is disabled.

**Syntax** `debug ppp [interface <ppp-interface-list>]`  
`no debug ppp [interface <ppp-interface-list>]`

| Parameter                                | Description  |
|--|--|
| <code>&lt;ppp-interface- list&gt;</code> | Specify a PPP interface or a range of PPP interfaces in the range <code>ppp&lt;0-255&gt;</code> . Use a hyphen between PPP interfaces to include all PPP interfaces in a given range, or use commas between PPP interfaces to specify non-contiguous PPP interfaces. |

**Default** No diagnostic messages are enabled for PPP debugging. PPP debugging is disabled by default.

**Mode** Global Configuration and Privileged Exec

**Usage notes** Debugging messages are sent to the logging system and can be viewed in log output, filtered in permanent or buffered logs, and viewed on the terminal using the [terminal monitor](#) command. See the status of PPP debugging with the [show debugging ppp](#) command.

Note that debugging output for PPP shows packet debugging and events debugging, see output below.

Note that disabling all debugging with the [no debug all](#) or the [undebug all](#) commands also disables PPP debugging configured with this command.

Note that the negated form of this command is an alias of the [undebug ppp](#) command.

**Examples** To enable PPP debugging on all PPP interfaces and send diagnostic messages to the system log, use the below command:

```
awplus# debug ppp
```

To enable PPP debugging on PPP interfaces `ppp0` through `ppp2` and display them on the console, use the below commands:

```
awplus# terminal monitor
```

```
awplus# debug ppp interface ppp0-ppp2
```

**Output of packet debugging**

Figure 13-1: Example output from the **debug ppp** command on the console

```
awplus#terminal monitor
awplus#debug ppp

05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.901] sent [IPCP
ConfReq id=0x1 <addr
0.0.0.0> <ms-dns1 0.0.0.0> <ms-dns2 0.0.0.0>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.901] sent [IPV6CP
ConfReq id=0x1
<addr fe80::eecd:6dff:fe3a:0d23>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.901] rcvd [LCP
ConfAck id=0x1 <magic
0xd9153444>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.919] rcvd [IPCP
ConfReq id=0x1 <addr
192.168.1.1>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.919] sent [IPCP
ConfAck id=0x1 <addr
192.168.1.1>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.919] rcvd [IPCP
ConfNak id=0x1 <addr
192.168.1.2> <ms-dns1 1.1.1.1> <ms-dns2 2.2.2.2>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.920] sent [IPCP
ConfReq id=0x2 <addr
192.168.1.2> <ms-dns1 1.1.1.1> <ms-dns2 2.2.2.2>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.921] rcvd [LCP
ProtRej id=0x2 80 57
01 01 00 0e 01 0a ee cd 6d ff fe 3a 0d 23]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.921] Protocol-Reject
for 'IPv6
Control Protocol' (0x8057) received
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.922] rcvd [IPCP
ConfAck id=0x2 <addr
192.168.1.2> <ms-dns1 1.1.1.1> <ms-dns2 2.2.2.2>]
02:25:35 awplus pppd[2388]: [ppp1] [02:25:35.990] sent [LCP
EchoReq id=0x3b
magic=0xe1e041db]
02:25:35 awplus pppd[2388]: [ppp1] [02:25:35.991] rcvd [LCP
EchoReq id=0x3b
magic=0xe3e331b1]
02:25:35 awplus pppd[2388]: [ppp1] [02:25:35.991] sent [LCP
EchoRep id=0x3b
magic=0xe1e041db]
02:25:35 awplus pppd[2388]: [ppp1] [02:25:35.992] rcvd [LCP
EchoRep id=0x3b
magic=0xe3e331b1]
```



**Output of event debugging**

Figure 13-2: Example output from the **debug ppp** command for a PPP interface

```
awplus#terminal monitor
awplus#debug ppp interface ppp0

05:35:43 awplus pppd[24767]: [ppp0] [05:35:43.710] using channel 1
05:35:43 awplus pppd[24767]: [ppp0] [05:35:43.712] Using interface
ppp0
05:35:43 awplus pppd[24767]: [ppp0] [05:35:43.712] Connect: ppp0
<--> hdlc0
05:35:46 awplus PPP: IPCP [ppp0]: add IP interface [IP-addr:
192.168.1.2, remote-IP:
192.168.1.1]
05:35:46 awplus PPP: IPCP [ppp0]: add IP interface [IP-addr:
192.168.1.2, mask: ]
05:35:46 awplus PPP: IPCP [ppp0]: add host route [peer-IP:
192.168.1.1]
05:35:47 awplus PPP: IPCP [ppp0]: add domain name server [DNS:
1.1.1.1]
05:35:47 awplus PPP: IPCP [ppp0]: add domain name server [DNS:
2.2.2.2]
```

To record messages relating to PPP packets in the buffered log, first configure a buffered log filter to select the messages using the commands:

```
awplus# configure terminal
awplus(config)# log buffered level debug program pppd
awplus(config)# end
```

Then configure PPP debugging, using the below command:

```
awplus# debug ppp
```

To disable PPP debugging for all PPP interfaces, use the below command:

```
awplus# no debug ppp
```

**Related commands**

- [terminal monitor](#)
- [encapsulation ppp](#)
- [no debug all](#)
- [ppp authentication](#)
- [show debugging ppp](#)
- [show interface \(PPP\)](#)
- [undebug all](#)

# encapsulation ppp

**Overview** Use this command to enable PPP encapsulation and create one or more PPP interfaces over Ethernet or a cellular interface.

Use the **no** variant of this command to disable PPP encapsulation and remove the specified PPP interface.

**Syntax** encapsulation ppp <index>  
no encapsulation ppp <index>

| Parameter | Description  |
|-----------|--|
| <index>   | The PPP interface index number in the range from 0 to 255. |

**Default** No PPP encapsulation or interfaces are configured by default.

**Mode** Interface Configuration mode for an Ethernet interface (e.g. **interface eth1**), or an Ethernet sub-interface (e.g. **interface eth1.1**), or a cellular interface (e.g. **interface cellular0**).

**Examples** To configure a PPP interface with index 0 for Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# encapsulation ppp 0
```

To shut down the ppp0 interface and remove it from Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# shutdown
awplus(config-if)# interface eth1
awplus(config-if)# no encapsulation ppp 0
```

**Related commands** [ppp service-name \(PPPoE\)](#)  
[show interface \(PPP\)](#)

# interface (PPP)

**Overview** Use this command to select a PPP interface to configure.

You need to use the [encapsulation ppp](#) command to enable PPP encapsulation and create PPP interfaces first.

**Syntax** `interface <PPP-interface-list>`

| Parameter                               | Description  |
|---|--|
| <code>&lt;PPP-interface-list&gt;</code> | The PPP interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"><li>• a PPP interface (e.g. ppp0)</li><li>• a continuous range of PPP interfaces, separated by a hyphen (e.g. ppp0-ppp2)</li><li>• a comma-separated non-continuous list of PPP interfaces (e.g. ppp0 , ppp2)</li></ul> The specified interfaces must exist. |

**Mode** Global Configuration

**Example** The following example shows how to enter Interface mode to configure a PPP interface.

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)#
```

**Related commands**

- [ip address \(IP Addressing and Protocol\)](#)
- [show interface](#)
- [show interface brief](#)

# ip address negotiated

**Overview** Use this command to obtain an IP address with the peer for a PPP interface via IPCP (Internet Protocol Control Protocol) address negotiation when configuring a PPP link for IP traffic.

Use the **no** variant of this command to remove IP address negotiation settings.

**Syntax** `ip address negotiated [<default-ip-address>]`  
`no ip address negotiated`

| Parameter                            | Description  |
|--------------------------------------|--|
| <code>&lt;default-ip-addr&gt;</code> | Specify an optional default IP address for use instead of an IP address assigned from the peer that is otherwise configured for a PPP interface. |

**Default** No IP address negotiation with the peer is configured by default.

**Mode** Interface Configuration for a PPP interface

**Usage notes** Use this command to enable the device to automatically negotiate an IP address for a PPP interface, and to enable all remote hosts to access the device using this IP address. When the peer does not send an IP address via IPCP negotiation, the specified default IP address will be used.

**Examples** To configure the PPP interface ppp0 to use IPCP to negotiate an IP address for itself, use the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip address negotiated
```

To configure the PPP interface ppp0 to a default IP address of 10.9.9.2, for use when the peer does not send an IP address via IPCP negotiation, use the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip address negotiated 10.9.9.2
```

To stop the PPP interface ppp0 from using IPCP to negotiate an IP address for itself, use the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip address negotiated
```

**Output** To verify IPCP address negotiation is configured on PPP interface ppp0, use the following command:

```
awplus# show running-config interface ppp0
```

Figure 13-3: Example output from **show running-config interface ppp0** to verify IPCP configuration:

```
!  
interface ppp0  
 ip address negotiated  
!
```

**Related commands**

- [show ip interface](#)
- [encapsulation ppp](#)
- [peer default ip address](#)
- [show running-config interface](#)

# ip tcp adjust-mss

**Overview** Use this command to set the Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

**Syntax** `ip tcp adjust-mss {<mss-size>|pmtu}`  
`no ip tcp adjust-mss`

| Parameter                     | Description  |
|-------------------------------|--|
| <code>&lt;mss-size&gt;</code> | <code>&lt;64-1460&gt;</code> Specifies the MSS size in bytes.          |
| <code>pmtu</code>             | Adjust TCP MSS automatically with respect to the MTU on the interface. |

**Default** The default setting allows a TCP server or a TCP client to set the MSS value for itself.

**Mode** Interface Configuration

**Usage notes** When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel
- VLAN

**Examples** To configure an MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ip tcp adjust-mss 1452
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip tcp adjust-mss
```

**Related  
commands**

[mtu \(PPP\)](#)  
[show interface](#)  
[show interface \(PPP\)](#)

**Command  
changes**

Version 5.4.8-2.1: interface tunnel example added

# ip unnumbered

**Overview** Use this command to borrow an IP address from the specified interface, on an unnumbered PPP interface.

Use the **no** variant of this command to remove the borrowed IP address.

**Syntax** `ip unnumbered <interface_name>`  
`no ip unnumbered`

| Parameter                           | Description  |
|-------------------------------------|--|
| <code>&lt;interface_name&gt;</code> | Name of the interface from which the IP address is to be borrowed. Valid interface types from which the IP address can be borrowed from are VLAN, ethernet, loopback and bridge. |

**Default** IP unnumbered is disabled by default.

**Mode** Interface Configuration for a PPP interface

**Usage notes** An unnumbered PPP interface can process IP packets without explicitly assigning an IP address. This is achieved by borrowing the primary IP address from the specified VLAN, ethernet, loopback or bridge interface.

**Examples** To borrow an IP address on unnumbered PPP from vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip address 6.6.6.6/24
awplus(config-if)# exit
awplus(config)# interface ppp0
awplus(config-if)# ip unnumbered vlan1
```

To remove the borrowed IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip unnumbered
```

To verify borrowed address is configured on PPP interface ppp0, use the following command:

```
awplus# show interface ppp0
```



Figure 13-4: Example output from a **show interface** ppp0 to verify PPP IP borrowing configuration:

```
awplus#show interface ppp0
Interface ppp0
  Link is UP, administrative state is UP
  Hardware is PPP
  Interface is unnumbered. Using IPv4 address of vlan1 (2.2.2.2)
  index 16778240 metric 1 mtu 1492
  <UP,POINT-TO-POINT,RUNNING,NOARP,MULTICAST>
  PPP is running over interface eth1
  LCP Opened IPCP Opened
  MRU(bytes): Local config 1492, Local negotiated 1492, Peer
  negotiated 1492
  Magic number: Local config ON, Local negotiated ON, Peer
  negotiated ON
  Authentication: Local config None, Local neg None, Peer neg CHAP
  IPv4 addresses: Local config 0.0.0.0
                  Local neg 2.2.2.2, Peer neg 1.1.1.1
  IPv6 Id Local config: 0000:0000:0000:0000
  PPPoE is using the default service
  SNMP link-status traps: Disabled
    input packets 2, bytes 20, dropped 0, multicast packets 0
    output packets 2, bytes 20, multicast packets 0 broadcast
  packets 0
  Time since last state change: 0 days 00:00:13
```

**Related commands** [show ip interface](#)  
[show running-config interface](#)

# ipv6 tcp adjust-mss

**Overview** Use this command to set the IPv6 Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

**Syntax** `ipv6 tcp adjust-mss {<mss-size>|pmtu}`  
`no ipv6 tcp adjust-mss`

| Parameter                     | Description  |
|-------------------------------|--|
| <code>&lt;mss-size&gt;</code> | <code>&lt;64-1460&gt;</code> Specifies the MSS size in bytes.          |
| <code>pmtu</code>             | Adjust TCP MSS automatically with respect to the MTU on the interface. |

**Default** The default setting allows a TCP server or a TCP client to set the MSS value for itself.

**Mode** Interface Configuration

**Usage notes** When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel
- VLAN

**Examples** To configure an IPv6 MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To configure an IPv6 MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To adjust IPv6 TCP MSS automatically with respect to the MTU on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ipv6 tcp adjust-mss pmtu
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 tcp adjust-mss
```

**Related  
commands**

[mtu \(PPP\)](#)  
[show interface](#)  
[show interface \(PPP\)](#)

**Command  
changes**

Version 5.4.8-2.1: interface tunnel example added

# keepalive (PPP)

**Overview** Use this command to enable LCP (Link Control Protocol) Echo keepalive request messages and change LCP echo parameters on a given PPP interface in Interface Configuration mode.

Use the **no** variant of this command to disable LCP Echo keepalive request messages on a given PPP interface in Interface Configuration mode. Note that disabling the sending of LCP Echo keepalive request messages does not stop a device responding to LCP Echo requests.

**Syntax** `keepalive [[interval <interval>] [attempts <attempt-limit>]]no keepalive`

| Parameter       | Description  |
|-----------------|--|
| <interval>      | Specify the interval in seconds in the range <1-600> seconds between LCP Echo keepalive request messages, for a PPP interface.<br>Default: 10  |
| <attempt-limit> | Specify the number of missing LCP Echo keepalive response messages, in the range <1-10> for a PPP interface, before the link is considered as being link down and link renegotiation starts to reestablish the link.<br>Default: 3 |

**Default** The sending of LCP Echo keepalive messages on a PPP interface is disabled by default. If no optional **interval** is specified then the default interval duration is configured to 10 seconds. If no optional **attempts** are specified then the default attempt limit is configured to 3 attempts.

**Mode** Interface Configuration for a PPP interface

**Example** To enable the device to send LCP Echo keepalive messages on the PPP interface `ppp0` with the default 10 second interval when no interval is specified and the default 3 attempts when no attempt is specified, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# keepalive
```

To enable the device to send LCP Echo keepalive messages on the PPP interface `ppp0` with double the default values for a 20 second interval and 6 attempts, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# keepalive interval 20 attempts 6
```

To disable the device from sending LCP Echo keepalive messages on the PPP interface `ppp0`, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no keepalive
```

**Related commands** [show running-config interface](#)

# mtu (PPP)

**Overview** Use this command to set the Maximum Transmission Unit (MTU) size for a PPP interface, where MTU is the maximum packet size that PPP interfaces can transmit.

Use the **no** variant of this command to remove a previously specified MTU size for a PPP interface, and restore the default MTU size (1492 bytes) for PPP interfaces.

**Syntax** `mtu <mtu-size>`  
`no mtu`

| Parameter                     | Description   |
|-------------------------------|---|
| <code>&lt;mtu-size&gt;</code> | <code>&lt;68-1492&gt;</code> Specifies the Maximum Transmission Unit (MTU) size in bytes, where 1492 bytes is the default MTU size for a PPPoE interface and 1500 bytes for PPP via other lower layer interface types. This allows for the 8-byte PPPoE header that is added to make up the total of a 1582 byte packet that matches the default MTU size for the Ethernet link.. |

**NOTE:** For PPPoE the minimum MTU value is 128.

**Default** The default MTU size is 1492 bytes for PPPoE interfaces. The MTU should be greater than, or equal to, the MSS.

**Mode** Interface Configuration for PPP interfaces.

**Usage notes** If a router receives an IPv4 packet for another PPP interface with an MTU size smaller than the packet size, and if the packet has the '**don't fragment**' bit set, then the switch will send an ICMP '**destination unreachable**' (3) packet type and a '**fragmentation needed and DF set**' (4) code back to the source.

See the `ip tcp adjust-mss` command to set the Maximum Segment Size (MSS) after first setting the MTU size.

**Examples** To configure an MTU size of 1492 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# mtu 1492
```

To restore the MTU size to the default MTU size of 1492 bytes on PPP interface ppp0, use the commands

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no mtu
```

**Related commands** `ip tcp adjust-mss`  
`show interface (PPP)`

# peer default ip address

**Overview** Use this command to set the default IP address assigned to the peer if required for a given PPP interface.

Use the optional **required** keyword with this command to specify that the peer must use this address for a given PPP interface, or drop the connection.

Use the **no** variant of this command to remove the previously specified peer default IP address for a given PPP interface.

**Syntax** peer default ip address <default-ip-address> [required]  
no peer default ip address

| Parameter            | Description   |
|----------------------|---|
| <default-ip-address> | Specify the IPv4 address to be assigned to the peer upon request.   |
| required             | Optionally specify the peer to acknowledge the default IP address, which requires the peer to use the address or drop the connection. |

**Default** No default IP address is configured to be assigned to the peer.

**Mode** Interface Configuration for a PPP interface

**Examples** To configure the PPP interface `ppp0` to assign the IP address of `192.168.0.1` to its peer upon request, use the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# peer default ip address 192.168.0.1
```

To configure the PPP interface `ppp0` to have the default peer IP address of `192.168.0.1`, and be required to use it or drop the connection, use the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# peer default ip address 192.168.0.1
required
```

To remove the default peer IP address of `192.168.0.1` from the PPP interface `ppp0`, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no peer default ip address
```

To verify the required peer default IP address 192.168.0.1 is configured on PPP interface ppp0, use the following command:

```
awplus# show running-config interface ppp0
```

### Output

**Table 1:** Example output from the **show running-config interface ppp0** command

```
awplus# show running-config interface ppp0
!
interface ppp0
  peer default ip address 192.168.0.1 required
!
```

**Related commands** [ip address negotiated](#)  
[show running-config interface](#)



# peer neighbor-route

**Overview** Use this command in Interface Configuration mode for a PPP interface to re-enable the creation of peer neighbor routes after the default behavior has been disabled.

Use the **no** form of this command in Interface Configuration mode for a PPP interface to disable the default behavior of creating a neighbor route for the peer.

**Syntax** peer neighbor-route  
no peer neighbor-route

**Default** A 32-bit host route (with a /32 mask) is created to the peer address on a PPP interface after PPP IPCP negotiation finishes.

**Usage notes** Use the **no** form of this command if the default behavior creates issues within your network. Use the [show ip route](#) command to validate the route behavior after issuing this command.

**Mode** Interface Configuration for a PPP interface

**Examples** To re-enable the default behavior for the PPP interface `ppp1`, where a 32-bit host route (with a /32 mask) is created to the peer address on a PPP interface after PPP IPCP negotiation finishes, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp1
awplus(config-if)# peer neighbor-route
```

To disable the default behavior for the PPP interface `ppp0`, to prevent a 32-bit host route being added to the IP router table, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no peer neighbor-route
```

**Related commands** [show interface \(PPP\)](#)  
[show ip route](#)

**Output** Figure 13-5: Example validation output from the **show interface** and **show ip route** commands issued before and after the **no peer neighbor-route** command (see IPv4 address in **show interface** output and see connected routes **show ip route** output):

```
awplus#show interface pppl
Interface pppl
  Scope: both
  Link is UP, administrative state is UP
  Hardware is PPP
  IPv4 address 4.1.1.2/32 pointopoint 4.1.1.1
  index 16778241 metric 1 mtu 1460
  <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
  VRF Binding: Not bound
  PPP is running over interface tunnell
  LCP Opened IPCP Opened
  L2TP session ID is 59451
  SNMP link-status traps: Disabled
    input packets 5, bytes 66, dropped 0, multicast packets 0
    output packets 4, bytes 46, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 00:02:24
awplus#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       *- candidate default

C       4.1.1.1/32 is directly connected, pppl
C       4.1.1.2/32 is directly connected, pppl
C       192.168.10.0/24 is directly connected, vlan1
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#interface pppl
awplus(config-if)#no peer neighbor-route
awplus(config-if)#exit
awplus(config)#exit
awplus#show interface pppl
Interface pppl
  Scope: both
  Link is UP, administrative state is UP
  Hardware is PPP
  IPv4 address 4.1.1.2/32
  index 16778241 metric 1 mtu 1460
  <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
  VRF Binding: Not bound
  PPP is running over interface tunnell
  LCP Opened IPCP Opened
  L2TP session ID is 6262
  SNMP link-status traps: Disabled
    input packets 5, bytes 66, dropped 0, multicast packets 0
    output packets 4, bytes 46, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 00:00:09
awplus#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default

C       4.1.1.2/32 is directly connected, pppl
C       192.168.10.0/24 is directly connected, vlan1
```

# ppp authentication

**Overview** Use this command in Interface Configuration mode for a PPP interface to configure PAP (Password Authentication Protocol), CHAP (Challenge Authentication Protocol), or EAP (Extensible Authentication Protocol).

Use the **no** form of this command in Interface Configuration mode for a PPP interface to disable all PAP, CHAP, and EAP authentication for a specified PPP interface.

**Syntax** `ppp authentication {eap|chap|pap}`  
`no ppp authentication`

| Parameter | Description   |
|-----------|---|
| eap       | Specify this parameter to enable EAP on a PPP interface   |
| chap      | Specify this parameter to enable CHAP on a PPP interface. |
| pap       | Specify this parameter to enable PAP on a PPP interface.  |

**Default** There is no PPP authentication protocol defined or configured to a PPP interface by default.

**Mode** Interface Configuration for a PPP interface

**Examples** To enable PPP PAP authentication on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication pap
```

To enable PPP CHAP authentication on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication chap
```

To enable PPP EAP authentication on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication eap
```

To attempt PPP EAP authentication, then fall back to PPP CHAP authentication if the attempt to enable PPP EAP authentication fails on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication eap chap
```

To attempt PPP CHAP authentication, then fall back to PPP PAP authentication if the attempt to enable PPP CHAP authentication fails on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication chap pap
```

To disable all PPP authentication on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp authentication
```

**Related commands**

- [ppp authentication refuse](#)
- [ppp hostname](#)
- [ppp password](#)
- [ppp username](#)

# ppp authentication refuse

**Overview** Use this command in Interface Configuration mode for a PPP interface to refuse EAP, CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) authentication from peers requesting it.

Use the **no** form of this command in Interface Configuration mode for a PPP interface to allow authentication from peers requesting it.

**Syntax** `ppp authentication refuse {eap|chap|pap}`  
`no ppp authentication refuse`

| Parameter | Description   |
|-----------|---|
| eap       | Use this parameter to specify the router will refuse LCP configuration requests containing the authentication protocol option with EAP received on this PPP interface.  |
| chap      | Use this parameter to specify the router will refuse LCP configuration requests containing the authentication protocol option with CHAP received on this PPP interface. |
| pap       | Use this parameter to specify the router will refuse LCP configuration requests containing the authentication protocol option with PAP on this PPP interface.           |

**Mode** Interface Configuration for a PPP interface

**Usage notes** This command specifies that EAP, CHAP or PAP authentication is disabled, so all requests by the peer for the user to authenticate using EAP, CHAP or PAP are refused.

**Examples** To refuse the use of PAP authentication if a peer requests PAP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication refuse pap
```

To refuse the use of CHAP authentication if a peer requests CHAP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication refuse chap
```

To refuse the use of EAP authentication if a peer requests EAP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication refuse eap
```

To allow the use of EAP, CHAP or PAP authentication if a peer requests EAP, CHAP or PAP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp authentication refuse
```

**Related commands** [ppp authentication](#)

# ppp hostname

**Overview** Use this command in Interface Configuration mode for a PPP interface to configure a unique identifier for that PPP authenticator. This is used by the authenticator to fill the Name field in a CHAP challenge packet, or is used to fill the Server Name field in an EAP SRP-SHA1 (Subtype 1 Request) packet. The hostname sent with PPP packet exchanges is normally the hostname of the router, as configured with the [hostname](#) command.

Use the **no** form of this command in Interface Configuration mode for a PPP interface to disable a configured alternate hostname and revert to using the hostname, as configured with the [hostname](#) command.

See the Usage section below for information about when you may want to specify another hostname, instead of the system hostname configured from the [hostname](#) command, using this command.

**Syntax** `ppp hostname <hostname>`  
`no ppp hostname <hostname>`

| Parameter                     | Description  |
|-------------------------------|--|
| <code>&lt;hostname&gt;</code> | Specify this parameter to use an alternate hostname for PPP EAP and CHAP authentication instead of the hostname specified by the <a href="#">hostname</a> command. The name can contain up to 255 characters. The name can contain any printable ASCII characters (ASCII 32-126). If the name contains the special characters backslash, double-quote or space, those characters should be escaped with a backslash. |

**Default** The default PPP hostname is the system hostname as specified with the [hostname](#) command.

**Mode** Interface Configuration for a PPP interface

**Usage notes** This command allows the PPP username that is sent to be independent of the router hostname for a specific PPP interface.

**Examples** To enable the use of the alternate hostname `remote_router` for PPP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp hostname remote_router
```

To disable the use of the alternate hostname `remote_router` for PPP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp hostname remote_router
```

**Related commands**

- [hostname](#)
- [ppp authentication](#)



# ppp ipcp dns

**Overview** Use this command to configure the primary and secondary DNS (Domain Name System) IP addresses for IPCP (Internet Protocol Control Protocol) on a given PPP interface.

Use the **no** variant of this command to remove the primary and secondary DNS IP addresses for IPCP on a given PPP interface, and remove any optional parameters configured for DNS.

**Syntax** `ppp ipcp dns [<primary> [<secondary>]][required|reject|request]`  
`no ppp ipcp dns`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;primary&gt;</code>   | Specify the primary DNS address for a given PPP interface to the peer.    |
| <code>&lt;secondary&gt;</code> | Specify the secondary DNS address for a given PPP interface to the peer.  |
| <code>required</code>          | Request DNS addresses from the peer, and close the link if none is given. |
| <code>reject</code>            | Reject negotiations with the peer (default).                              |
| <code>request</code>           | Request DNS addresses from the peer.                                      |

**Default** By default no IPCP DNS server request is sent to the peer.

**Mode** Interface Configuration

**Usage notes** Use the optional parameters to configure PPP IPCP DNS options for accepting, rejecting or requesting DNS addresses from the peer. Use the optional primary and secondary or primary only DNS server address placeholders to specify DNS server addresses to the peer.

The no variant of this command also stops IPCP DNS request messages being sent to the peer.

**Examples** To configure the PPP interface `ppp0` to require a DNS IP address from the peer, and close the link if a DNS IP address is not given, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns required
```

To configure the PPP interface `ppp0` to require a DNS IP address from the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns request
```

To configure the PPP interface `ppp0` to reject a DNS IP address from the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns reject
```

To configure the PPP interface `ppp0` to supply primary and secondary DNS server addresses to the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns 10.1.1.2 10.1.1.3
```

To configure the PPP interface `ppp0` to supply a primary but not a secondary DNS server address to the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns 10.1.1.2
```

**Related  
commands**

[ip address negotiated](#)  
[peer default ip address](#)  
[peer neighbor-route](#)  
[show running-config interface](#)

# ppp ipcp dns suffix-list

**Overview** Use this command to configure a suffix-list to be associated with DNS name-servers learned over the PPP connection.

Use the **no** variant of this command to remove the suffix-list.

**Syntax** `ppp ipcp dns suffix-list <domain-list-name>`  
`no ppp ipcp dns suffix-list`

| Parameter                             | Description                     |
|---------------------------------------|---------------------------------|
| <code>&lt;domain-list-name&gt;</code> | The name of the DNS domain-list |

**Mode** Interface Configuration

**Usage notes** A PPP connection can be configured to learn DNS servers from the remote peer by using the command `ppp ipcp dns` command.

This command allows a user to associate a domain-list to be used to match against the suffixes of incoming DNS requests. For example, a customer branch office may have a router that is used to give remote-access to their head office, over which they learn the IP address of the head office's DNS server. A domain list can be created that contains a suffix used for services internal to that company, for example, "example.lc". This domain-list is associated as a suffix-list to the PPP connection. So when the PPP connection is completed with the head office, users at the branch office that browse to "intranet.example.lc" will have the DNS request forwarded to the DNS server learned over the PPP connection. Without having the suffix-list configured, the DNS request for "intranet.example.lc" would instead be sent to the primary DNS server, which is likely to be the branch office's ISP, and they will simply respond with a negative reply, because .example.lc is not a globally routable domain.

**Examples** At a branch office, to direct DNS lookups for domains with suffixes of "engineering.acme" or "intranet.acme" to an internal corporate name-server run at head-office that was learned over a PPP connection, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list corporatedomains
host(config-domain-list)# description Our internal network
domains; do not send DNS requests to internet
host(config-domain-list)# domain engineering.acme
host(config-domain-list)# domain intranet.acme
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns required
awplus(config-if)# ppp ipcp dns suffix-list corporatedomains
```

**Related commands** [ip dns forwarding domain-list](#)  
[ppp ipcp dns](#)

# ppp ipcp ip-override

**Overview** Use this command to override the IP address negotiated via IPCP with peer and use the statically configured address on a given PPP interface.

Use the **no** variant of this command to use any address negotiated with the peer via IPCP on a given PPP interface.

**Syntax** `ppp ipcp ip-override`  
`no ppp ipcp ip-override`

**Default** By default the address is negotiated with the peer via IPCP.

**Mode** Interface Configuration

**Examples** To override the IP address negotiated with the peer via IPCP and use statically configured address on interface ppp0, use the commands below:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip address 192.168.1.100/24
awplus(config-if)# ppp ipcp ip-override
```

**Related commands** [show running-config interface](#)

# ppp password

**Overview** Use this command in Interface Configuration mode for a PPP interface to configure a PPP secret password to be used in response to a challenge from an unknown remote peer.

Use the **no** form of this command in Interface Configuration mode for a PPP interface to disable a configured PPP secret password.

**Syntax** `ppp password <password>`  
`no ppp password`

| Parameter                     | Description  |
|-------------------------------|--|
| <code>&lt;password&gt;</code> | Specify this parameter to configure a PPP secret password to be used in response to an unknown remote peer. You can use any printable characters, including spaces. A password can contain up to 255 printable characters. |

**Default** There is no PPP password defined or configured to a PPP interface by default.

**Mode** Interface Configuration for a PPP interface

**Examples** To enable the use of the PPP secret password `bobs_secret` for PPP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp password bobs_secret
```

To disable the use of the PPP secret password `bobs_secret` for PPP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp password
```

**Related commands** [ppp authentication](#)  
[ppp username](#)

# ppp service-name (PPPoE)

**Overview** This command configures the PPPoE service name used to select a service from an access concentrator. This can only be applied when the PPP interface has been configured over an underlying eth interface.

Use the **no** variant of this command to set the service name for the connection back to the default (unset).

**Syntax** `ppp service-name <service-name>`  
`no ppp service-name`

| Parameter                         | Description   |
|-----------------------------------|---|
| <code>&lt;service-name&gt;</code> | Specifies the PPPoE service name to select from an access concentrator. The service-name is 1 to 18 characters long, is case-sensitive, and for a PPPoE client is usually supplied by the ISP.<br>The name can contain any printable ASCII characters (ASCII 32-126). If the name contains the special characters backslash, double-quote or space, those characters should be escaped with a backslash.<br>The default is no service name. |

**Default** The default option is not to specify a service name. This results in a connection to the default service specified by the access concentrator.

**Mode** Interface Configuration for a PPP interface

**Usage notes** You can only apply a single service name to each PPPoE interface.

**Examples** To connect to a service called "Internet", use the command:

```
awplus(config)# interface ppp0  
awplus(config-if)# ppp service-name Internet
```

**Related commands** [encapsulation ppp](#)  
[show interface \(PPP\)](#)

# ppp timeout idle

**Overview** Use this command to specify an idle time when a PPP connection is disconnected. Use the **no** variant of this command to reset the idle time to the default of 60 seconds.

**Syntax** `ppp timeout idle <0-99999>`  
`no ppp timeout idle`

| Parameter                    | Description  |
|------------------------------|--|
| <code>&lt;0-99999&gt;</code> | The time in seconds before the idle timeout disconnects. If this is not specified the default value of 60 seconds is used. |

**Default** PPP timeout idle is not set and the PPP Dial on Demand feature is disabled. If no idle time is set, the default value of 60 seconds is used.

**Mode** Interface Configuration

**Usage notes** This command allows an idle timer to disconnect a PPP connection after a specified time. The timer is reset upon either ingress or regress user traffic. Non-user traffic such as Link Control Protocol (LCP) keepalives and Network Control Protocol (NCP) negotiation packets do not reset the idle timer.

**Examples** To set the idle time to 30 seconds, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp timeout idle
30
```

To disable the use of the timer and disable the PPP Dial on Demand feature, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp timeout
idle 30
```

**Validation Commands** `show running-config interface`



# ppp username

**Overview** This command creates or modifies a username for a PPP user on a configured PPP interface.

**Syntax** `ppp username <username>`  
`no ppp username`

| Parameter                     | Description   |
|-------------------------------|---|
| <code>&lt;username&gt;</code> | Specify a login name for the user. The name can contain up to 255 characters.<br>The name can contain any printable ASCII characters (ASCII 32-126). If the name contains the special characters backslash, double-quote or space, those characters should be escaped with a backslash. |

**Default** There is no default PPP username defined or configured to a PPP interface.

**Mode** Interface Configuration for a PPP interface.

**Examples** To create the PPP username bob, for the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp username bob
```

To remove the PPP username bob, for the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp username
```

**Related commands** [ppp authentication](#)  
[ppp password](#)

# show debugging ppp

**Overview** Use this command to display PPP debug settings for optionally specified PPP interfaces. If no PPP interfaces are specified then PPP debug settings are shown for all available PPP interfaces.

**Syntax** `show debugging ppp [interface <0-255>]`

| Parameter | Description  |
|-----------|--|
| <0-255>   | Specify a PPP interface or a range of PPP interfaces in the range <code>ppp&lt;0-255&gt;</code> . Use a hyphen between PPP interfaces to include all PPP interfaces in a given range, or use commas between PPP interfaces to specify non-contiguous PPP interfaces. |

**Mode** Privileged Exec

**Examples** The following example shows how to display PPP debug information for PPP interface `ppp0`:

```
awplus# show debugging ppp interface ppp0
```

The following example shows how to display PPP debug information for PPP interface `ppp0` through `ppp2`:

```
awplus# show debugging ppp interface ppp0-ppp2
```

The following example shows how to display PPP debug information for PPP interface `ppp0` and `ppp2`:

```
awplus# show debugging ppp interface ppp0,ppp2
```

The following example shows how to display PPP debug information for all available PPP interfaces:

```
awplus# show debugging ppp
```

Figure 13-6: Example output from the **show debugging ppp** command

```
awplus# show debugging ppp
PPP debugging status:
  PPP debug on interface ppp0: enabled
  PPP debug on interface ppp1: disabled
```

**Related commands**

- [debug ppp](#)
- [no debug all](#)
- [undebug all](#)
- [show interface \(PPP\)](#)

# show interface (PPP)

**Overview** Use this command to display configuration and status information for a configured PPP (Point-to-Point) interface.

**Syntax** `show interface ppp<ppp_index>`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;ppp_index&gt;</code> | Display configuration and status information for the specified and configured PPP interface (0 to 255). |

**Mode** User Exec and Privileged Exec

**Usage notes** See the [show interface brief](#) command for brief interface, configuration and status information.

Note the negotiated options, including those for DNS addresses, are shown in console output:

- Local DNS addresses as displayed in console output are provided from the peer.
- Peer DNS addresses as displayed in console output are provided to the peer.
- Only Peer DNS addresses or Local DNS addresses are shown, but not both.
- Echo Request Timer value as displayed in console output is the local setting.

**Example** The following example shows how to display the configuration and status information for a configured PPP interface named `ppp0`.

```
awplus# show interface ppp0
```

Figure 13-7: Example output from the **show interface** command for a PPPoE interface

```
awplus#show interface ppp0

Interface ppp0
  Scope: both
  Link is UP, administrative state is UP
  Hardware is PPP
  IPv4 address 10.1.0.2/32
  IPv6 address fe80::200:cdff:fe28:8a1/10
  index 16778440 metric 1
  <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
  VRF Binding: Not bound
  PPP is running over interface eth0
  PPPoE is using the default service
  SNMP link-status traps: Disabled
    input packets 12, bytes 458, dropped 0, multicast packets 0
    output packets 6, bytes 122, multicast packets 0 broadcast
  packets 0
  Time since last state change: 0 days 00:01:57
```

Figure 13-8: Example output from the **show interface ppp1** command showing negotiated DNS addresses, where the peer provided the DNS information (see the **Local DNS addresses** field output below):

```
awplus#sh interface ppp1
Interface ppp1
  Scope: both
  Link is UP, administrative state is UP
  Hardware is PPP
  IPv4 address 192.168.1.1/30 pointopoint 192.168.1.2
  IPv6 address fe80::200:cdf:fe28:89f/10
  index 16778241 metric 1 mtu 1460
  <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
  VRF Binding: Not bound
  PPP is running over interface tunnel1
  LCP Opened IPCP Opened IPV6CP Opened
  MRU(bytes): Local config 1460, Local negotiated 1460, Peer
  negotiated 1460
  Magic number: Local config ON, Local negotiated ON, Peer
  negotiated ON
  Authentication: Local config None, Local neg None, Peer neg None
  Echo Request Timer (seconds): 10
  IPv4 addresses: Local config 192.168.1.1, Peer neg 192.168.1.2
  IPv6 interface ID: Local eecd:6dff:fe3a:0d18, Peer neg
  eecd:6dff:fe3a:0d18
  Local DNS addresses: 192.168.60.1, 192.168.60.2
  L2TP session ID is 15288
  SNMP link-status traps: Disabled
    input packets 5, bytes 96, dropped 0, multicast packets 0
    output packets 5, bytes 96, multicast packets 0 broadcast
  packets 0
  Time since last state change: 0 days 00:06:29
awplus#
```

Figure 13-9: Example output from the **show interface ppp1** command showing negotiated DNS addresses, where the peer was provided with DNS information (see the **Peer DNS addresses** field output below):

```
awplus#sh interface ppp1
Interface ppp1
  Scope: both
  Link is UP, administrative state is UP
  Hardware is PPP
  IPv4 address 192.168.1.1/30 pointopoint 192.168.1.2
  IPv6 address fe80::200:cdff:fe28:89f/10
  index 16778241 metric 1 mtu 1460
  <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
  VRF Binding: Not bound
  PPP is running over interface tunnel1
  LCP Opened IPCP Opened IPV6CP Opened
  MRU(bytes): Local config 1460, Local negotiated 1460, Peer
  negotiated 1460
  Magic number: Local config ON, Local negotiated ON, Peer
  negotiated ON
  Authentication: Local config None, Local neg None, Peer neg None
  Echo Request Timer (seconds): 10
  IPv4 addresses: Local config 192.168.1.1, Peer neg 192.168.1.2
  IPv6 interface ID: Local eecd:6dff:fe3a:0d18, Peer neg
  eecd:6dff:fe3a:0d18
  Peer DNS addresses: 1.1.1.1, 2.2.2.2
  L2TP session ID is 15288
  SNMP link-status traps: Disabled
    input packets 5, bytes 96, dropped 0, multicast packets 0
    output packets 5, bytes 96, multicast packets 0 broadcast
  packets 0
  Time since last state change: 0 days 00:06:29
awplus#
```

**Related  
commands**

- [encapsulation ppp](#)
- [ppp service-name \(PPPoE\)](#)
- [show interface](#)
- [show interface brief](#)

# undebug ppp

**Overview** Use this command to disable PPP protocol debugging on the specified PPP interface or interfaces. If no PPP interface is specified then PPP debugging for all PPP interfaces is disabled.

This command has the same functionality as the **no** variant of the [debug ppp](#) command.

**Syntax** undebug ppp [*interface <ppp-interface-list>*]

| Parameter                         | Description  |
|-----------------------------------|--|
| <i>&lt;ppp-interface-list&gt;</i> | Specify a PPP interface or a range of PPP interfaces in the range <code>ppp&lt;0-255&gt;</code> . Use a hyphen between PPP interfaces to include all PPP interfaces in a given range, or use commas between PPP interfaces to specify non-contiguous PPP interfaces. |

**Default** No diagnostic messages are enabled for PPP debugging. PPP debugging is disabled by default.

**Mode** Privileged Exec

**Usage notes** Note that this command is an alias of the negated form of the [debug ppp](#) command.

**Examples** To disable PPP debugging for all PPP interfaces, enter the below command:

```
awplus# undebug ppp
```

To disable PPP debugging for PPP interfaces `ppp0`, enter the below command:

```
awplus# undebug ppp interface ppp0
```

To disable PPP debugging for PPP interfaces `ppp0` through `ppp2`, enter the below command:

```
awplus# undebug ppp interface ppp0-ppp2
```

To disable PPP debugging for PPP interfaces `ppp0` and `ppp2`, enter the below command:

```
awplus# undebug ppp interface ppp0,ppp2
```

**Related commands**

- [debug ppp](#)
- [no debug all](#)
- [show debugging ppp](#)
- [undebug all](#)

# Part 3: Routing



# 14

# IP Addressing and Protocol Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure various IP features, including the following protocols:

- Address Resolution Protocol (ARP)

For more information, see the [IP Feature Overview and Configuration Guide](#).

- Command List**
- [“arp-aging-timeout”](#) on page 475
  - [“arp”](#) on page 476
  - [“arp log”](#) on page 477
  - [“arp opportunistic-nd”](#) on page 480
  - [“arp-reply-bc-dmac”](#) on page 481
  - [“clear arp-cache”](#) on page 482
  - [“debug ip packet interface”](#) on page 483
  - [“ip address \(IP Addressing and Protocol\)”](#) on page 485
  - [“ip directed-broadcast”](#) on page 486
  - [“ip forward-protocol udp”](#) on page 488
  - [“ip gratuitous-arp-link”](#) on page 490
  - [“ip helper-address”](#) on page 492
  - [“ip limited-local-proxy-arp”](#) on page 494
  - [“ip local-proxy-arp”](#) on page 496
  - [“ip proxy-arp”](#) on page 497
  - [“ip redirects”](#) on page 498
  - [“ip tcp synack-retries”](#) on page 499
  - [“ip tcp timeout established”](#) on page 500

- [“ip unreachable”](#) on page 501
- [“local-proxy-arp”](#) on page 503
- [“optimistic-nd”](#) on page 504
- [“ping”](#) on page 505
- [“show arp”](#) on page 506
- [“show debugging ip packet”](#) on page 507
- [“show ip flooding-next hops”](#) on page 508
- [“show ip interface”](#) on page 509
- [“show ip sockets”](#) on page 510
- [“show ip traffic”](#) on page 513
- [“tcpdump”](#) on page 515
- [“traceroute”](#) on page 516
- [“undebug ip packet interface”](#) on page 517

# arp-aging-timeout

**Overview** This command sets a timeout period on dynamic ARP entries associated with a specific interface. If your device stops receiving traffic for the host specified in a dynamic ARP entry, it deletes the ARP entry from the ARP cache after this timeout is reached.

Your device times out dynamic ARP entries to ensure that the cache does not fill with entries for hosts that are no longer active. Static ARP entries are not aged or automatically deleted.

By default the time limit for dynamic ARP entries is 300 seconds on all interfaces. The **no** variant of this command sets the time limit to the default of 300 seconds.

**Syntax** `arp-aging-timeout <0-432000>`  
`no arp-aging timeout`

| Parameter                     | Description                    |
|-------------------------------|--------------------------------|
| <code>&lt;0-432000&gt;</code> | The timeout period in seconds. |

**Default** 300 seconds (5 minutes)

**Mode** Interface Configuration for a VLAN interface.

**Example** To set the ARP entries on interface vlan1 to time out after two minutes, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# arp-aging-timeout 120
```

**Related commands** [clear arp-cache](#)  
[show arp](#)

# arp

**Overview** This command adds a static ARP entry to the ARP cache. This is typically used to add entries for hosts that do not support ARP or to speed up the address resolution function for a host. The ARP entry must not already exist. Use the **alias** parameter to allow your device to respond to ARP requests for this IP address.

The **no** variant of this command removes the static ARP entry. Use the [clear arp-cache](#) command to remove the dynamic ARP entries in the ARP cache.

**Syntax** `arp <ip-addr> <mac-address> [<port-number>] [alias]`  
`no arp <ip-addr>`

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;ip-addr&gt;</code>     | The IPv4 address of the device you are adding as a static ARP entry.  |
| <code>&lt;mac-address&gt;</code> | The MAC address of the device you are adding as a static ARP entry, in hexadecimal notation with the format HHHH.HHHH.HHHH.               |
| <code>&lt;port-number&gt;</code> | The port number associated with the IP address. Specify this when the IP address is part of a VLAN.                                       |
| <code>alias</code>               | Allows your device to respond to ARP requests for the IP address. Proxy ARP must be enabled on the interface before using this parameter. |

**Mode** Global Configuration

**Examples** To add the IP address 10.10.10.9 with the MAC address 0010.2533.4655 into the ARP cache, and have your device respond to ARP requests for this address, use the commands:

```
awplus# configure terminal
awplus(config)# arp 10.10.10.9 0010.2355.4566 alias
```

**Related commands** [clear arp-cache](#)  
[ip proxy-arp](#)  
[show arp](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# arp log

**Overview** This command enables the logging of dynamic and static ARP entries in the ARP cache. The ARP cache contains mappings of device ports, VLAN IDs, and IP addresses to physical MAC addresses for hosts.

This command can display the MAC addresses in the ARP log either using the notation HHHH.HHHH.HHHH, or using the IEEE standard hexadecimal notation (HH-HH-HH-HH-HH-HH).

Use the **no** variant of this command to disable the logging of ARP entries.

**Syntax** `arp log [mac-address-format ieee]`  
`no arp log [mac-address-format ieee]`

| Parameter                            | Description  |
|--------------------------------------|--|
| <code>mac-address-format ieee</code> | Display the MAC address in the standard IEEE format (HH-HH-HH-HH-HH-HH), instead of displaying the MAC address with the format HHHH.HHHH.HHHH. |

**Default** The ARP logging feature is disabled by default.

**Mode** Global Configuration

**Usage notes** You have the option to change how the MAC address is displayed in the ARP log message. The output can either use the notation HHHH.HHHH.HHHH or HH-HH-HH-HH-HH-HH.

Enter **arp log** to use HHHH.HHHH.HHHH notation.

Enter **arp log mac-address-format ieee** to use HH-HH-HH-HH-HH-HH notation.

Enter **no arp log mac-address-format ieee** to revert from HH-HH-HH-HH-HH-HH to HHHH.HHHH.HHHH.

Enter **no arp log** to disable ARP logging.

To display ARP log messages use the command **show log | include ARP\_LOG**.

**Examples** To enable ARP logging and specify that the MAC address in the log message is displayed in HHHH.HHHH.HHHH notation, use the following commands:

```
awplus# configure terminal
awplus(config)# arp log
```

To disable ARP logging on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log
```

To enable ARP logging and specify that the MAC address in the log message is displayed in the standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH), use the following commands:

```
awplus# configure terminal
awplus(config)# arp log mac-address-format ieee
```

To leave ARP logging enabled, but stop using HH-HH-HH-HH-HH-HH format and use HHHH.HHHH.HHHH format instead, use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log mac-address-format ieee
```

To display ARP log messages, use the following command:

```
awplus# show log | include ARP_LOG
```

**Output** Figure 14-1: Output from **show log | include ARP\_LOG** after enabling ARP logging using **arp log**. Note that this output uses HHHH.HHHH.HHHH format.

```
awplus#configure terminal
awplus(config)#arp log
awplus(config)#exit
awplus#show log | include ARP_LOG
2018 Oct 6 06:21:01 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 add
0013.4078.3b98 (192.168.2.4)
2018 Oct 6 06:22:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 del
0013.4078.3b98 (192.168.2.4)
2018 Oct 6 06:23:26 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 add
0030.940e.136b (192.168.2.20)
2018 Oct 6 06:23:30 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Figure 14-2: Output from **show log | include ARP\_LOG** after enabling ARP logging using **arp log mac-address format ieee**. Note that this output uses HH-HH-HH-HH-HH-HH format.

```
awplus#configure terminal
awplus(config)#arp log mac-address-format ieee
awplus(config)#exit
awplus#show log | include ARP_LOG
2018 Oct 6 06:25:28 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 add
00-17-9a-b6-03-69 (192.168.2.12)
2018 Oct 6 06:25:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 add
00-03-37-6b-a6-a5 (192.168.2.10)
2018 Oct 6 06:26:53 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 del
00-30-94-0e-13-6b (192.168.2.20)
2018 Oct 6 06:27:31 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 del
00-17-9a-b6-03-69 (192.168.2.12)
2018 Oct 6 06:28:09 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 del
00-03-37-6b-a6-a5 (192.168.2.10)
2018 Oct 6 06:28:14 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

The following table lists the parameters in output of the **show log | include ARP\_LOG** command. The ARP log message format is:

```
<date> <time> <severity> <hostname> <program-name>  
ARP_LOG <port-number> <vid> <operation> <MAC> <IP>
```

Table 14-1: Parameters in the output from **show log | include ARP\_LOG**

| Parameter     | Description  |
|---------------|--|
| ARP_LOG       | Indicates that ARP log entry information follows.  |
| <port-number> | Indicates device port number for the ARP log entry.  |
| <vid>         | Indicates the VLAN ID for the ARP log entry.   |
| <operation>   | Indicates "add" if the ARP log entry displays an ARP addition. Indicates "del" if the ARP log entry displays an ARP deletion.  |
| <MAC>         | Indicates the MAC address for the ARP log entry, either in the default hexadecimal notation (HHHH.HHHH.HHHH) or in the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) as specified with the <b>arp log mac-address-format ieee</b> command. |
| <IP>          | Indicates the IP address for the ARP log entry.  |

**Related commands** [show log](#)  
[show running-config](#)

# arp opportunistic-nd

**Overview** Use this command to enable opportunistic neighbor discovery for the global ARP cache. This command changes the behavior for unsolicited ARP packet forwarding on the device.

Use the **no** variant of this command to disable opportunistic neighbor discovery for the global ARP cache.

**Syntax** `arp opportunistic-nd`  
`no arp opportunistic-nd`

**Default** Opportunistic neighbor discovery is disabled by default.

**Mode** Global Configuration

**Usage notes** When opportunistic neighbor discovery is enabled, the device will reply to any received unsolicited ARP packets (but not gratuitous ARP packets). The source MAC address for the unsolicited ARP packet is added to the ARP cache, so the device forwards the ARP packet. When opportunistic neighbor discovery is disabled, the source MAC address for the ARP packet is not added to the ARP cache, so the ARP packet is not forwarded by the device.

**Examples** To enable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# arp opportunistic-nd
```

To disable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# no arp opportunistic-nd
```

**Related commands** [ipv6 opportunistic-nd](#)  
[show arp](#)  
[show running-config interface](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.



# arp-reply-bc-dmac

**Overview** Use this command to allow processing of ARP replies that arrive with a broadcast destination MAC (ffff.ffff.ffff). This makes neighbors reachable if they send ARP responses that contain a broadcast destination MAC.

Use the **no** variant of this command to turn off processing of ARP replies that arrive with a broadcast destination MAC.

**Syntax** `arp-reply-bc-dmac`  
`no arp-reply-bc-dmac`

**Default** By default, this functionality is disabled.

**Mode** Interface Configuration for VLAN, Eth and bridge interfaces

**Example** To allow processing of ARP replies that arrive on vlan1 with a broadcast destination MAC, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# arp-reply-bc-dmac
```

**Related commands** [clear arp-cache](#)  
[show arp](#)

# clear arp-cache

**Overview** This command deletes dynamic ARP entries from the ARP cache. You can optionally specify the IPv4 address of an ARP entry to be cleared from the ARP cache.

**Syntax** `clear arp-cache [<ip-address>]`

| Parameter                 | Description  |
|---------------------------|--|
| <i>&lt;ip-address&gt;</i> | The IPv4 address of an ARP entry that is to be cleared from the ARP cache. |

**Mode** Privileged Exec

**Usage notes** To display the entries in the ARP cache, use the [show arp](#) command. To remove static ARP entries, use the no variant of the [arp](#) command.

**Example** To clear all dynamic ARP entries, use the command:

```
awplus# clear arp-cache
```

To clear all dynamic ARP entries associated with the IPv4 address 192.168.1.1, use the command:

```
awplus# clear arp-cache 192.168.1.1
```

**Related commands** [arp](#)  
[show arp](#)

# debug ip packet interface

**Overview** The **debug ip packet interface** command enables IP packet debug and is controlled by the **terminal monitor** command.

If the optional **icmp** keyword is specified then ICMP packets are shown in the output.

The **no** variant of this command disables the **debug ip interface** command.

**Syntax** `debug ip packet interface {<interface-name>|all} [address <ip-address>|verbose|hex|arp|udp|tcp|icmp]`  
`no debug ip packet interface [<interface-name>]`

| Parameter    | Description  |
|--------------|--|
| <interface>  | Specify a single Layer 3 interface name (not a range of interfaces)<br>This keyword can be specified as either all or as a single Layer 3 interface to show debugging for either all interfaces or a single interface. |
| all          | Specify all Layer 3 interfaces on the device.  |
| <ip-address> | Specify an IPv4 address.<br>If this keyword is specified, then only packets with the specified IP address as specified in the ip-address placeholder are shown in the output.  |
| verbose      | Specify <b>verbose</b> to output more of the IP packet.<br>If this keyword is specified then more of the packet is shown in the output.  |
| hex          | Specify <b>hex</b> to output the IP packet in hexadecimal.<br>If this keyword is specified, then the output for the packet is shown in hex.  |
| arp          | Specify <b>arp</b> to output ARP protocol packets.<br>If this keyword is specified, then ARP packets are shown in the output.  |
| udp          | Specify <b>udp</b> to output UDP protocol packets.<br>If this keyword is specified then UDP packets are shown in the output.   |
| tcp          | Specify <b>tcp</b> to output TCP protocol packets.<br>If this keyword is specified, then TCP packets are shown in the output.  |
| icmp         | Specify <b>icmp</b> to output ICMP protocol packets.<br>If this keyword is specified, then ICMP packets are shown in the output.   |

**Mode** Privileged Exec and Global Configuration

**Examples** To turn on ARP packet debugging on vlan1, use the command:

```
awplus# debug ip packet interface vlan1 arp
```

To turn off IP packet interface debugging on interface vlan1, use the command:

```
awplus# no debug ip packet interface vlan1
```

To turn on all packet debugging on all interfaces on the device, use the command:

```
awplus# debug ip packet interface all
```

To turn off IP packet interface debugging on all interfaces, use the command:

```
awplus# no debug ip packet interface
```

To turn on TCP packet debugging on vlan1 and IP address 192.168.2.4, use the command:

```
awplus# debug ip packet interface vlan1 address 192.168.2.4 tcp
```

**Related  
commands**

[no debug all](#)

[show debugging ip dns forwarding](#)

[tcpdump](#)

[terminal monitor](#)

[undebug ip packet interface](#)

# ip address (IP Addressing and Protocol)

**Overview** This command sets a static IP address on an interface.  
The **no** variant of this command removes the IP address from the interface.

**Syntax** `ip address <ip-addr/prefix-length>`  
`no ip address [<ip-addr/prefix-length>]`

| Parameter                                  | Description  |
|--|--|
| <code>&lt;ip-addr/prefix-length&gt;</code> | The IPv4 address and prefix length you are assigning to the interface. |

**Mode** Interface Configuration for a VLAN interface, a local loopback interface, a PPP interface, or a tunnel.

**Examples** To add the IP address 10.10.10.50/24 to the interface `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip address 10.10.10.50/24
```

To add the IP address 10.10.11.50/24 to the local loopback interface `lo`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.11.50/24
```

To add the IP address 10.10.11.50/24 to the PPP interface `ppp0`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip address 10.10.11.50/24
```

To add the IP address 10.10.11.50/24 to the tunnel `tunnel0`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# ip address 10.10.11.50/24
```

**Related commands** [interface \(to configure\)](#)  
[show ip interface](#)  
[show running-config interface](#)

# ip directed-broadcast

**Overview** Use this command to enable flooding of directed broadcast packets into a directly connected subnet. If this command is configured on 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, a local loopback interface, or a PPP interface.

**Usage notes** IP directed-broadcast is enabled and disabled per VLAN interface. When enabled a directed broadcast packet is forwarded to an enabled VLAN interface if received on another subnet.

An IP directed broadcast is an IP packet whose destination address is a broadcast address for some IP subnet, but originates from a node that is not itself part of that destination subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is flooded as a broadcast on the destination subnet.

The **ip directed-broadcast** command controls the flooding of directed broadcasts when they reach target subnets. The command affects the final transmission of the directed broadcast on its destination subnet. It does not affect the transit unicast routing of IP directed broadcasts. If directed broadcast is enabled for an interface, incoming directed broadcast IP packets intended for the subnet assigned to interface will be flooded as broadcasts on that subnet.

If the **no ip directed-broadcast** command is configured for an interface, directed broadcasts destined for the subnet where the interface is attached will be dropped instead of broadcast.

**Examples** To enable the flooding of broadcast packets out via the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip directed-broadcast
```

To disable the flooding of broadcast packets via PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip directed-broadcast
```

**Related commands**

- [ip forward-protocol udp](#)
- [ip helper-address](#)
- [show running-config](#)

# 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](http://www.iana.org)) for a list of assigned UDP port numbers for protocols to forward using **ip forward-protocol udp**.

Use the **no** variant of this command to remove a port number from the list of destination port numbers that are used as the criterion for deciding if a given UDP broadcast should be forwarded to the IP helper address(es).

**Syntax** `ip forward-protocol udp <port>`  
`no ip forward-protocol udp <port>`

| Parameter | Description      |
|-----------|------------------|
| <port>    | UDP Port Number. |

**Default** The **ip forward-protocol udp** command is not enabled by default.

**Mode** Global Configuration

**Usage notes** Combined with the **ip helper-address** command in interface mode, the **ip forward-protocol udp** command in Global Configuration mode allows control of which protocols (destination port numbers) are forwarded. The **ip forward-protocol udp** command configures protocols for forwarding, and the **ip helper-address** command configures the destination address(es).

**NOTE:**

*The types of UDP broadcast packets that the device will forward are ONLY those specified by the **ip forward-protocol** command(s). There are no other UDP packet types that the IP helper process forwards by default.*

**Examples** To configure forwarding of packets on a UDP port, use the following commands:

```
awplus# configure terminal
awplus(config)# ip forward-protocol udp <port>
```

To delete a UDP port from the UDP ports that the device forwards, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip forward-protocol udp <port>
```



**Related  
commands** [ip helper-address](#)  
[ip directed-broadcast](#)  
[show running-config](#)

# ip 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   |
|-----------|---|
| <0-300>   | Specify the minimum time between sequences of Gratuitous ARPs and the fixed time between Gratuitous ARPs occurring in a sequence, in seconds.<br>0 disables the sending of Gratuitous ARP packets.<br>The default is 8 seconds. |

**Default** The default Gratuitous ARP time limit for all switchports is 8 seconds.

**Mode** Global Configuration

**Usage** Every switchport will send a sequence of 3 Gratuitous ARP packets to each VLAN that the switchport is a member of, whenever the switchport moves to the forwarding state. The first Gratuitous ARP packet is sent 1 second after the switchport becomes a forwarding switchport. The second and third Gratuitous ARP packets are each sent after the time period specified by the Gratuitous ARP time limit.

Additionally, the Gratuitous ARP time limit specifies the minimum time between the end of one Gratuitous ARP sequence and the start of another Gratuitous ARP sequence. When a link is flapping, the switchport's state is set to forwarding several times. The Gratuitous ARP time limit is imposed to prevent Gratuitous ARP packets from being sent undesirably often.

**Examples** To disable the sending of Gratuitous ARP packets, use the commands :

```
awplus# configure terminal
awplus(config)# ip gratuitous-arp-link 0
```

To restrict the sending of Gratuitous ARP packets to one every 20 seconds, use the commands:

```
awplus# configure terminal  
awplus(config)# ip gratuitous-arp-link 20
```

**Validation  
Commands** `show running-config`

# ip helper-address

**Overview** Use this command to add a forwarding destination address for IP Helper to enable forwarding of User Datagram Protocol (UDP) broadcasts on an interface.

Use the **no** variant of this command to disable the forwarding of broadcast packets to specific addresses.

**Syntax** `ip helper-address <ip-addr>`  
`no ip helper-address <ip-addr>`

| Parameter                    | Description                                      |
|------------------------------|--|
| <code>&lt;ip-addr&gt;</code> | Forwarding destination IP address for IP Helper. |

**Default** The destination address for the **ip helper-address** command is not configured by default.

**Mode** Interface Configuration for a VLAN interface, a local loopback interface, or a PPP interface.

**Usage notes** Combined with the **ip forward-protocol udp** command in global configuration mode, the **ip helper-address** command in interface mode allows control of which protocols (destination port numbers) are forwarded. The **ip forward-protocol udp** command configures protocols for forwarding, and the **ip helper-address** command configures the destination address(es).

The destination address can be a unicast address or a subnet broadcast address. The UDP destination port is configured separately with the **ip forward-protocol udp** command. If multiple destination addresses are registered then UDP packets are forwarded to each IP address added to an IP Helper. Up to 32 destination addresses may be added using IP Helper.

The device will only forward the types of UDP broadcast packets that are specified by the **ip forward-protocol** command(s). The device does not forward any other UDP packet types by default.

The **ip helper-address** command does not support BOOTP / DHCP Relay. The **service dhcp-relay** command must be used instead. For this reason, you may not configure UDP ports 67 and 68 with the **ip forward-protocol** command.

See the [IP Feature Overview and Configuration Guide](#) for more information about DHCP Relay.

**Examples** The following example defines IPv4 address 192.168.1.100 as an IP Helper destination address to which to forward UDP broadcasts received on ppp0:

```
awplus# configure terminal
awplus(config)# interface ppp0
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 ppp0:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip helper-address 192.168.1.100
```

**Related commands**

- [ip forward-protocol udp](#)
- [ip directed-broadcast](#)
- [show running-config](#)

# ip limited-local-proxy-arp

**Overview** Use this command to enable local proxy ARP, but only for a specified set of IP addresses. This makes the device respond to ARP requests for those IP addresses when the addresses are reachable via the interface you are configuring.

To specify the IP addresses, use the command [local-proxy-arp](#).

Use the **no** variant of this command to disable limited local proxy ARP. This stops your device from intercepting and responding to ARP requests for the specified hosts. This allows the hosts to use MAC address resolution to communicate directly with one another.

**Syntax** `ip limited-local-proxy-arp`  
`no ip limited-local-proxy-arp`

**Default** Limited local proxy ARP is disabled by default.

**Mode** Interface Configuration

**Usage** Limited local proxy ARP supports Static NAT configurations in which the NAT configuration's public address is different to the ethernet interface's address.

On such ethernet interfaces, the device needs to respond to ARP requests for the public address so that it will receive packets targeted at that address.

Limited local proxy ARP makes this possible. It is especially useful when you have a number of 1-1 NAT configurations and each public address falls within the public interface's subnet. If you enable limited local proxy ARP on the public interface and specify suitable addresses, the device will respond to ARP requests for those addresses, as long as the addresses are routed out the interface the ARP requests are received on. The device responds with its own MAC address.

**Example** The following configuration snippet shows how to use limited local proxy ARP, if you are using NAT for an HTTP server with an address of 172.22.0.3 connected via eth1, and eth1 has an address of 172.22.0.1:

```
! Create a private zone for the HTTP server with address 172.22.200.3:
zone private
network vlan1
ip subnet 172.22.200.0/24
host http_server
ip address 172.22.200.3
!
! Create a public zone for the HTTP server with address 172.22.0.3:
zone public
network eth1
ip subnet 0.0.0.0/0 interface eth1
host http_server
ip address 172.22.0.3
!
! Create a NAT rule to map from the public to the private zone:
nat
rule 10 portfwd http from public.eth1 to public.eth1.http_server with dst
private.vlan1.http_server
enable
!
! Configure eth1. It has a different public address than the HTTP server:
interface eth1
ip limited local-proxy-arp
ip address 172.22.0.1/24
!
! Configure vlan1:
interface vlan1
ip address 172.22.200.5/24
!
! Tell the device to respond to ARPs for the HTTP server public address:
local-proxy-arp 172.22.0.3/32
```

**Related commands** [ip local-proxy-arp](#)  
[local-proxy-arp](#)

# ip local-proxy-arp

**Overview** This command allows you to stop MAC address resolution between hosts within a private VLAN edge interface. Local Proxy ARP works by intercepting ARP requests between hosts within a subnet and responding with your device's own MAC address details instead of the destination host's details. This stops hosts from learning the MAC address of other hosts within its subnet through ARP requests.

Local Proxy ARP ensures that devices within a subnet cannot send traffic that bypasses Layer 3 routing on your device. This lets you monitor and filter traffic between hosts in the same subnet, and enables you to have control over which hosts may communicate with one another.

When Local Proxy ARP is operating on an interface, your device does not generate or forward any ICMP-Redirect messages on that interface. This command does not enable proxy ARP on the interface; see the [ip proxy-arp](#) command for more information on enabling proxy ARP.

The **no** variant of this command disables Local Proxy ARP to stop your device from intercepting and responding to ARP requests between hosts within a subnet. This allows the hosts to use MAC address resolution to communicate directly with one another. Local Proxy ARP is disabled by default.

**Syntax** `ip local-proxy-arp`  
`no ip local-proxy-arp`

**Default** Local proxy ARP is disabled by default

**Mode** Interface Configuration for a VLAN interface or a local loopback interface.

**Examples** To enable your device to apply Local Proxy ARP on the interface `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip local-proxy-arp
```

To disable your device to apply Local Proxy ARP on the interface `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip local-proxy-arp
```

**Related commands** [ip proxy-arp](#)  
[show arp](#)

[show running-config](#)



# ip proxy-arp

**Overview** This command enables Proxy ARP responses to ARP requests on an interface. When enabled, your device intercepts ARP broadcast packets and substitutes its own physical address for that of the remote host. By responding to the ARP request, your device ensures that subsequent packets from the local host are directed to its physical address, and it can then forward these to the remote host.

Your device responds only when it has a specific route to the address being requested, excluding the interface route that the ARP request arrived from. It ignores all other ARP requests. See the [ip local-proxy-arp](#) command about enabling your device to respond to other ARP messages.

The **no** variant of this command disables Proxy ARP responses on an interface. Proxy ARP is disabled by default.

**Syntax** `ip proxy-arp`  
`no ip proxy-arp`

**Default** Proxy ARP is disabled by default.

**Mode** Interface Configuration for a VLAN interface or a local loopback interface.

**Examples** To enable your device to Proxy ARP on the interface vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip proxy-arp
```

To disable your device to Proxy ARP on the interface vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip proxy-arp
```

**Related commands** [arp](#)  
[ip local-proxy-arp](#)  
[show arp](#)  
[show running-config](#)

# ip redirects

**Overview** This command enables the device to send ICMP redirects.

Use the **no** variant of this command to stop the device from sending ICMP redirects.

**Syntax** `ip redirects`  
`no ip redirects`

**Default** ICMP redirects are disabled by default.

**Mode** Global Configuration.

**Usage notes** ICMP redirect messages are used to notify hosts that a better route is available to a destination.

ICMP redirects are used when a packet is routed into the device on the same interface that the packet is routed out of the device. ICMP redirects are only sent to packet sources that are directly connected to the device.

**Examples** To enable the switch to send ICMP redirects, use the following commands:

```
awplus# configure terminal
awplus(config)# ip redirects
```

To stop the switch from sending ICMP redirects, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip redirects
```

# ip tcp synack-retries

**Overview** Use this command to specify how many times the switch will retry sending a SYN ACK for a TCP connection for which it has received a SYN but not an ACK. Such connections are called half-open TCP connections. This command allows you to influence how long half-open TCP connections take to time out.

Use the **no** variant of this command to return to the default setting of 5 retries.

**Syntax** `ip tcp synack-retries <0-255>`  
`no ip tcp synack-retries`

| Parameter | Description                                  |
|-----------|--|
| <0-255>   | Number of times to retry sending the SYN ACK |

**Default** 5 retries

**Mode** Global Configuration

**Usage notes** The following table shows the approximate correlation between the number of retries and the time half-open TCP connections take to time out.

| Number of retries | Approximate lower bound for the timeout |
|-------------------|---|
| 0 retries         | 1 second                                |
| 1 retry           | 3 seconds                               |
| 2 retries         | 7 seconds                               |
| 3 retries         | 15 seconds                              |
| 4 retries         | 31 seconds                              |
| 5 retries         | 63 seconds                              |

**Example** To retry twice, which leads to a timeout of approximately 7 seconds, use the commands:

```
awplus# configure terminal  
awplus(config)# ip tcp synack-retries 2
```

**Related commands** [show running-config](#)

**Command changes** Version 5.4.7-0.2: command added

# ip tcp timeout established

**Overview** Use this command to set the idle timeout for all established TCP connections. Use the **no** variant of this command to set the idle timeout back to the default of 3600 seconds.

**Syntax** `ip tcp timeout established <1-31536000>`  
`no ip tcp timeout established`

| Parameter                       | Description  |
|---------------------------------|--|
| <code>&lt;1-31536000&gt;</code> | Idle timeout for established TCP connections in seconds from 1 to 3153600. |

**Default** 3600 seconds (1 hour)

**Mode** Global Configuration

**Usage notes** By default, when a TCP session is successfully established through the firewall, when the session goes idle, it automatically times out of the firewall connection tracking table after 3600 seconds. In some situations it may be beneficial to time out unused established TCP sessions earlier.

For example, in a busy environment where there is an excessive number of sessions being established, the firewall connection tracking table could become oversubscribed, with new connections being blocked until older sessions are timed out.

**Example** To set a non-default TCP session timeout for established idle sessions of 1800 seconds (30 minutes), use the commands:

```
awplus# configure terminal
awplus(config)# ip tcp timeout established 1800
```

**Example** To set the TCP session timeout for established idle sessions back to the default setting of 3600 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip tcp timeout established
```

**Related commands** [show running-config](#)

**Command changes** Version 5.4.6-1.1: command added

# ip unreachables

**Overview** Use this command to enable ICMP (Internet Control Message Protocol) type 3, destination unreachable, messages.

Use the **no** variant of this command to disable destination unreachable messages. This prevents an attacker from using these messages to discover the topology of a network.

**Syntax** `ip unreachables`  
`no ip unreachables`

**Default** Destination unreachable messages are enabled by default.

**Mode** Global Configuration

**Usage notes** When a device receives a packet for a destination that is unreachable it returns an ICMP type 3 message, this message includes a reason code, as per the table below. An attacker can use these messages to obtain information regarding the topology of a network. Disabling destination unreachable messages, using the **no ip unreachables** command, secures your network against this type of probing.

**NOTE:** *Disabling ICMP destination unreachable messages breaks applications such as traceroute and Path MTU Discovery (PMTUD), which depend on these messages to operate correctly.*

Table 14-2: ICMP type 3 reason codes and description

| Code | Description [RFC]                                  |
|------|--|
| 0    | Network unreachable [RFC792]                       |
| 1    | Host unreachable [RFC792]                          |
| 2    | Protocol unreachable [RFC792]                      |
| 3    | Port unreachable [RFC792]                          |
| 4    | Fragmentation required, and DF flag set [RFC792]   |
| 5    | Source route failed [RFC792]                       |
| 6    | Destination network unknown [RFC1122]              |
| 7    | Destination host unknown [RFC1122]                 |
| 8    | Source host isolated [RFC1122]                     |
| 9    | Network administratively prohibited [RFC768]       |
| 10   | Host administratively prohibited [RFC869]          |
| 11   | Network unreachable for Type of Service [RFC908]   |
| 12   | Host unreachable for Type of Service [RFC938]      |
| 13   | Communication administratively prohibited [RFC905] |

Table 14-2: ICMP type 3 reason codes and description (cont.)

| Code | Description [RFC]                     |
|------|---------------------------------------|
| 14   | Host Precedence Violation [RFC1812]   |
| 15   | Precedence cutoff in effect [RFC1812] |

**Example** To disable destination unreachable messages, use the commands

```
awplus# configure terminal  
awplus(config)# no ip unreachable
```

To enable destination unreachable messages, use the commands

```
awplus# configure terminal  
awplus(config)# ip unreachable
```

# local-proxy-arp

**Overview** Use this command to specify an IP subnet for use with limited local proxy ARP. When limited local proxy ARP is enabled with the command `ip limited-local-proxy-arp`, the device will respond to ARP requests for addresses in that subnet.

Use the **no** variant of this command to stop specifying a subnet for use with limited local proxy ARP.

**Syntax** `local-proxy-arp [<ip-add/mask>]`  
`no local-proxy-arp [<ip-add/mask>]`

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;ip-add/mask&gt;</code> | The IP subnet to use with limited local proxy ARP, in dotted decimal format (A.B.C.D/M). To specify a single IP address, use a 32-bit mask. |

**Default** No subnets are specified for use with limited local proxy ARP.

**Mode** Global Configuration

**Example** To specify limited local proxy ARP for the address 172.22.0.3, use the following commands:

```
awplus# configure terminal
awplus(config)# local-proxy-arp 172.22.0.3/32
```

This is part of a configuration snippet that shows how to use limited local proxy ARP with static NAT. See the command `ip limited-local-proxy-arp` for the whole example.

**Related commands** `ip limited-local-proxy-arp`

# optimistic-nd

**Overview** Use this command to enable the optimistic neighbor discovery feature for both IPv4 and IPv6.

Use the **no** variant of this command to disable the optimistic neighbor discovery feature.

**Syntax** `optimistic-nd`  
`no optimistic-nd`

**Default** The optimistic neighbor discovery feature is enabled by default.

**Mode** Interface Configuration for a VLAN interface.

**Usage notes** The optimistic neighbor discovery feature allows the device, after learning an IPv4 or IPv6 neighbor, to refresh the neighbour before it is deleted from the ARP or neighbour tables. The optimistic neighbor discovery feature enables the device to sustain L3 traffic switching to a neighbor without interruption.

If a neighbor receiving optimistic neighbor solicitations does not answer optimistic neighbor solicitations with neighbor advertisements, then the device puts the neighbour entry into the "stale" state, and subsequently deletes it from the L3 switching tables.

**Examples** To enable the optimistic neighbor discovery feature on vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# optimistic-nd
```

To disable the optimistic neighbor discovery feature on vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no optimistic-nd
```

**Related commands** [show running-config](#)



# ping

**Overview** This command sends a query to another IPv4 host (send Echo Request messages).

**Syntax** ping [ip] <host> [broadcast] [df-bit {yes|no}] [interval <0-128>] [pattern <hex-data-pattern>] [repeat {<1-2147483647>|continuous}] [size <36-18024>] [source <ip-addr>] [timeout <1-65535>] [tos <0-255>]

| Parameter                  | Description  |
|----------------------------|--|
| <host>                     | The destination IP address or hostname.  |
| broadcast                  | Allow pinging of a broadcast address.  |
| df-bit                     | Enable or disable the do-not-fragment bit in the IP header.  |
| interval <0-128>           | Specify the time interval in seconds between sending ping packets. The default is 1. You can use decimal places to specify fractions of a second. For example, to ping every millisecond, set the interval to 0.001. |
| pattern <hex-data-pattern> | Specify the hex data pattern.  |
| repeat                     | Specify the number of ping packets to send.  |
| <1-2147483647>             | Specify repeat count. The default is 5.  |
| continuous                 | Continuous ping  |
| size <36-18024>            | The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).  |
| source <ip-addr>           | The IP address of a configured IP interface to use as the source in the IP header of the ping packet.  |
| timeout <1-65535>          | The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.   |
| tos <0-255>                | The value of the type of service in the IP header.   |

**Mode** User Exec and Privileged Exec

**Example** To ping the IP address 10.10.0.5 use the following command:

```
awplus# ping 10.10.0.5
```

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# show arp

**Overview** Use this command to display entries in the ARP routing and forwarding table—the ARP cache contains mappings of IP addresses to physical addresses for hosts. To have a dynamic entry in the ARP cache, a host must have used the ARP protocol to access another host.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show arp

**Mode** User Exec and Privileged Exec

**Usage notes** Running this command with no additional parameters will display all entries in the ARP routing and forwarding table.

**Example** To display all ARP entries in the ARP cache, use the following command:

```
awplus# show arp
```

**Output** Figure 14-3: Example output from the **show arp** command

```
awplus#show arp
IP Address      LL Address      Interface  Port           Type
192.168.27.10   192.168.4.1     vlan1      port1.0.1      dynamic
192.168.27.100 0000.daaF.cd24  vlan1      port1.0.2      dynamic
192.168.1.100   192.168.20.1   vlan1      port1.0.3      static
```

**Table 15:** Parameters in the output of the **show arp** command

| Parameter  | Meaning   |
|------------|---|
| IP Address | IP address of the network device this entry maps to.  |
| LL Address | Hardware address of the network device.   |
| Interface  | Interface over which the network device is accessed.  |
| Port       | Physical port that the network device is attached to.   |
| Type       | Whether the entry is a static or dynamic entry. Static entries are added using the <a href="#">arp</a> command. Dynamic entries are learned from ARP request/reply message exchanges. |

**Related commands** arp  
clear arp-cache

**Command changes** Version 5.4.9-0.1: Link layer addresses now shown as the hardware address (MAC Address output parameter has been renamed to LL Address).

# show debugging ip packet

**Overview** Use this command to see what debugging is turned on for IP interfaces. IP interface debugging is set using the **debug ip packet interface** command.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show debugging ip packet

**Mode** User Exec and Privileged Exec

**Example** To display the IP interface debugging status when the terminal monitor is off, use the commands:

```
awplus# terminal no monitor
awplus# show debugging ip packet
```

**Output** Figure 14-4: Example output from the **show debugging ip packet** command with **terminal monitor** off

```
awplus#terminal no monitor
awplus#show debugging ip packet
IP debugging status:
interface all tcp (stopped)
interface vlan1 arp verbose (stopped)
```

**Example** To display the IP interface debugging status when the terminal monitor is on, use the commands:

```
awplus# terminal monitor
awplus# show debugging ip packet
```

**Output** Figure 14-5: Example output from the **show debugging ip packet** command with **terminal monitor** on

```
awplus#terminal monitor
awplus#show debugging ip packet
IP debugging status:
interface all tcp (running)
interface vlan1 arp verbose (running)
```

**Related commands** [debug ip packet interface](#)  
[terminal monitor](#)

# show ip flooding-nextops

**Overview** Use this command to display the static and dynamic ARP entries in the ARP cache that flood packets to multiple ports.

**Syntax** `show ip flooding-nextops`

**Mode** User Exec and Privileged Exec

**Example** To display all of the flooding nexthop entries in the ARP cache, use the command:

```
awplus# show ip flooding-nextops
```

**Output** Figure 14-6: Example output from **show ip flooding-nextops**

```
awplus#show ip flooding-nextops
```

| IP Address  | MAC Address    | Interface | Flooding Mode | Type   |
|-------------|----------------|-----------|---------------|--------|
| 11.11.11.10 | 0300.0000.0011 | vlan1     | port-group    | static |

**Related commands** [show arp](#)

**Command changes** Version 5.4.8-2.1: command added

# show ip interface

**Overview** Use this command to display information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip interface [<interface-list>] [brief]`

| Parameter                           | Description   |
|-------------------------------------|---|
| <code>&lt;interface-list&gt;</code> | The interfaces to display information about. An interface-list can be: <ul style="list-style-type: none"><li>• a PPP interface (e.g. ppp0)</li><li>• an Eth interface (e.g. eth1)</li><li>• vlan1</li><li>• a bridge interface (e.g. br0)</li><li>• a tunnel interface (e.g. tunnel0)</li><li>• a WWAN interface (e.g. wwan0)</li><li>• the loopback interface (lo)</li><li>• a continuous range of interfaces, separated by a hyphen (e.g. ppp2-4)</li><li>• a comma-separated list (e.g. ppp0,ppp2-4). Do not mix interface types in a list.</li></ul> The specified interfaces must exist. |

**Mode** User Exec and Privileged Exec

**Examples** To show brief information for the assigned IP address for interface port1.0.2 use the command:

```
awplus# show ip interface port1.0.2 brief
```

To show the IP addresses assigned to vlan1, use the command:

```
awplus# show ip interface vlan1 brief
```

To show the IP addresses assigned to ppp0, use the command:

```
awplus# show ip interface ppp0 brief
```

**Output** Figure 14-7: Example output from the **show ip interface brief** command

| Interface | IP-Address  | Status   | Protocol |
|-----------|-------------|----------|----------|
| port1.0.1 | unassigned  | admin up | down     |
| ...       |             |          |          |
| vlan1     | 192.168.1.1 | admin up | running  |
| ...       |             |          |          |

# show ip sockets

**Overview** Use this command to display information about the IP or TCP sockets that are present on the device. It includes TCP and UDP listen sockets, and displays the associated IP address and port.

The information displayed for established TCP sessions includes the remote IP address, port, and session state. Raw IP protocol listen socket information is also displayed for protocols such as VRRP and ICMP6, which are configured to receive IP packets with the associated protocol number.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip sockets`

**Mode** Privileged Exec

**Usage notes** Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

Note that this command does not display sockets that are used internally for exchanging data between the various processes that exist on the device and are involved in its operation and management. It only displays sockets that are present for the purposes of communicating with other external devices.

**Example** To display IP sockets currently present on the device, use the command:

```
awplus# show ip sockets
```

**Output** Figure 14-8: Example output from **show ip sockets**

```
Socket information

Not showing 40 local connections
Not showing 7 local listening ports
```

| Typ | Local Address   | Remote Address | State  |
|-----|-----------------|----------------|--------|
| tcp | 0.0.0.0:111     | 0.0.0.0:*      | LISTEN |
| tcp | 0.0.0.0:80      | 0.0.0.0:*      | LISTEN |
| tcp | 0.0.0.0:23      | 0.0.0.0:*      | LISTEN |
| tcp | 0.0.0.0:443     | 0.0.0.0:*      | LISTEN |
| tcp | 0.0.0.0:4743    | 0.0.0.0:*      | LISTEN |
| tcp | 0.0.0.0:873     | 0.0.0.0:*      | LISTEN |
| tcp | :::23           | :::*           | LISTEN |
| udp | 0.0.0.0:111     | 0.0.0.0:*      |        |
| udp | 226.94.1.1:5405 | 0.0.0.0:*      |        |
| udp | 0.0.0.0:161     | 0.0.0.0:*      |        |
| udp | :::161          | :::*           |        |
| raw | 0.0.0.0:112     | 0.0.0.0:*      | 112    |
| raw | :::58           | :::*           | 58     |
| raw | :::112          | :::*           | 112    |

Table 14-1: Parameters in the output from **show ip sockets**

| Parameter  | Description  |
|--|--|
| Not showing<br><number><br>local<br>connections        | This field refers to established sessions between processes internal to the device, that are used in its operation and management. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.   |
| Not showing<br><number><br>local<br>listening<br>ports | This field refers to listening sockets belonging to processes internal to the device, that are used in its operation and management. They are not available to receive data from other devices. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.  |
| Typ  | This column displays the type of the socket. Possible values for this column are:<br>tcp : IP Protocol 6<br>udp : IP Protocol 17<br>raw : Indicates that socket is for a non port-orientated protocol (i.e. a protocol other than TCP or UDP) where all packets of a specified IP protocol type are accepted. For raw socket entries the protocol type is indicated in subsequent columns.   |
| Local<br>Address                                       | For TCP and UDP listening sockets this shows the destination IP address and destination TCP or UDP port number for which the socket will receive packets. The address and port are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 or :: for IPv6. For active TCP sessions the IP address will display which of the devices addresses the session was established with. For raw sockets this displays the IP address and IP protocol for which the socket will accept IP packets. The address and protocol are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 and :: for IPv6. IP Protocol assignments are described at: <a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a> |

Table 14-1: Parameters in the output from **show ip sockets** (cont.)

| Parameter      | Description   |
|----------------|---|
| Remote Address | For TCP and UDP listening sockets this shows the source IP address (either IPv4 or IPv6) and source TCP or UDP port number for which the socket will accept packets. The address and port are separated by ':'. If the socket will accept packets addressed from any IP address, the IP address will be 0.0.0.0 for IPv4. This is the usual case for a listening socket. Normally for a listen socket any source port will be accepted. This is indicated by '*'. For active TCP sessions the IP address will display the remote address and port the session was established with. For raw sockets the entry in this column will be 0.0.0.0: for IPv4. |
| State          | This column shows the state of the socket. For TCP sockets this shows the state of the TCP state machine. For UDP sockets this column is blank. For raw sockets it contains the IP protocol number. The possible TCP states are:<br>LISTEN<br>SYN-SENT<br>SYN-RECEIVED<br>ESTABLISHED<br>FIN-WAIT-1<br>FIN-WAIT-2<br>CLOSE-WAIT<br>CLOSING<br>LAST-ACK<br>TIME-WAIT<br>CLOSED<br>RFC793 contains the TCP state machine diagram with Section 3.2 describing each of the states.  |



# show ip traffic

**Overview** Use this command to display statistics regarding IP traffic sent and received by all interfaces on the device, showing totals for IP and IPv6 and then broken down into sub-categories such as TCP, UDP, ICMP and their IPv6 equivalents when appropriate.

For information on filtering and saving command output, see 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 14-9: Example output from the **show ip traffic** command

```
awplus#show ip traffic
IP:
    168475 packets received
    168475 delivered
    208099 sent
    35 dropped due to missing route
    22646409 bytes received
    126783216 bytes sent
    InCsumErrors 0
    InNoECTPkts 168475
    InECT1Pkts 0
    InECT0Pkts 0
    InCEPkts 0
    In107 Destination Unreachable
    Out11 Destination Unreachable
IPv6:
    14 packets received
    14 received packets delivered
    18 packets transmitted
...
ICMP6:
    4 messages sent
...
UDP6:
    Udp6RcvbufErrors 0
...
UDPLite6:
    UdpLite6RcvbufErrors 0
...
```

```
TCP:
    8 remote connections established
...
UDP:
    79797 datagrams received
...
UDPLite:
    InCsumErrors 0
...
```

# tcpdump

**Overview** Use this command to start a tcpdump, which gives the same output as the Unix-like **tcpdump** command to display TCP/IP traffic. Press <ctrl> + c to stop a running tcpdump.

**Syntax** `tcpdump <line>`

| Parameter                 | Description  |
|---------------------------|--|
| <code>&lt;line&gt;</code> | Specify the dump options. For more information on the options for this placeholder see <a href="http://www.tcpdump.org/tcpdump_man.html">http://www.tcpdump.org/tcpdump_man.html</a> |

**Mode** Privileged Exec

**Example** To start a tcpdump running to capture IP packets, enter the command:

```
awplus# tcpdump ip
```

**Output** Figure 14-10: Example output from the **tcpdump** command

```
03:40:33.221337 IP 192.168.1.1 > 224.0.0.13: PIMv2, Hello,
length: 34
1 packets captured
2 packets received by filter
0 packets dropped by kernel
```

**Related commands** [debug ip packet interface](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# traceroute

**Overview** Use this command to trace the route to the specified IPv4 host.

**Syntax** `traceroute {<ip-addr>|<hostname>}`

| Parameter                     | Description   |
|-------------------------------|---|
| <code>&lt;ip-addr&gt;</code>  | The destination IPv4 address. The IPv4 address uses the format A.B.C.D. |
| <code>&lt;hostname&gt;</code> | The destination hostname.   |

**Mode** User Exec and Privileged Exec

**Example** `awplus# traceroute 10.10.0.5`

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# undebug ip packet interface

**Overview** This command applies the functionality of the no `debug ip packet interface` command.

# 15

# Domain Name Service (DNS) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure Domain Name Service (DNS) features, including the following:

- DNS client
- DNS forwarding (DNS relay)
- Domain lists
- DDNS (Dynamic Domain Name System)

For more information about DNS and DDNS for AR-Series Firewalls, see the [Domain Name System \(DNS\) for AlliedWare Plus AR-Series Firewalls Feature Overview and Configuration Guide](#).

- Command List**
- “accept-invalid-sslcert” on page 520
  - “clear ip dns forwarding cache” on page 521
  - “ddns enable” on page 522
  - “ddns-update-method” on page 523
  - “ddns-update now” on page 524
  - “debug ddns” on page 525
  - “debug ip dns forwarding” on page 526
  - “description (Domain List)” on page 527
  - “domain (Domain List)” on page 528
  - “host-name (DDNS)” on page 529
  - “ip ddns-update-method” on page 530
  - “ip dns forwarding” on page 531
  - “ip dns forwarding cache” on page 532
  - “ip dns forwarding dead-time” on page 533

- [“ip dns forwarding domain-list”](#) on page 534
- [“ip dns forwarding retry”](#) on page 535
- [“ip dns forwarding source-interface”](#) on page 536
- [“ip dns forwarding timeout”](#) on page 537
- [“ip domain-list”](#) on page 538
- [“ip domain-lookup”](#) on page 539
- [“ip domain-name”](#) on page 541
- [“ip name-server”](#) on page 542
- [“ip name-server preferred-order”](#) on page 544
- [“ipv6 ddns-update-method”](#) on page 545
- [“password \(DDNS\)”](#) on page 546
- [“ppp ipcp dns”](#) on page 547
- [“ppp ipcp dns suffix-list”](#) on page 549
- [“retry-interval \(DDNS\)”](#) on page 551
- [“show ddns-update-method status”](#) on page 552
- [“show debugging ip dns forwarding”](#) on page 553
- [“show hosts”](#) on page 554
- [“show ip dns forwarding”](#) on page 555
- [“show ip dns forwarding cache”](#) on page 556
- [“show ip dns forwarding server”](#) on page 557
- [“show ip domain-list”](#) on page 558
- [“show ip domain-name”](#) on page 559
- [“show ip name-server”](#) on page 560
- [“suppress-ipv4-updates \(DDNS\)”](#) on page 561
- [“undebg \(DDNS\)”](#) on page 562
- [“update-interval \(DDNS\)”](#) on page 563
- [“update-url \(DDNS\)”](#) on page 564
- [“use-ipv4-for-ipv6-updates \(DDNS\)”](#) on page 567
- [“username \(DDNS\)”](#) on page 568

# accept-invalid-sslcert

**Overview** Use this command to tell the dynamic DNS client to connect to an HTTPS server even if the server is producing an invalid SSL certificate (because it is self-signed, for a different host, expired, etc.).

Use the **no** variant of this command to return to the default.

**Syntax** `accept-invalid-sslcert`  
`no accept-invalid-sslcert`

**Default** Not set

**Mode** Dynamic DNS Update Method Configuration Mode

**Example** If the HTTPS server you are using for the dynamic DNS configuration "test" does not have a valid SSL certificate, then use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method test
awplus(config-ddns-update-method)# accept-invalid-sslcert
```

**Command changes** Version 5.5.0-0.1: command added



# clear ip dns forwarding cache

**Overview** Use this command to clear the DNS Relay name resolver cache.

**Syntax** `clear ip dns forwarding cache`

**Mode** Privileged Exec

**Examples** To clear all cached data, use the command:

```
awplus# clear ip dns forwarding cache
```

**Related commands** [ip dns forwarding cache](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# ddns enable

**Overview** Use this command to enable DDNS updates.  
Use the **no** variant of this command to disable DDNS updates.

**Syntax** `ddns enable`  
`no ddns enable`

**Default** Disabled

**Mode** Global Configuration

**Example** To globally enable DDNS updates, use the commands:

```
awplus# configure terminal
awplus(config)# ddns enable
```

To globally disable DDNS updates, use the commands:

```
awplus# configure terminal
awplus(config)# no ddns enable
```

**Related commands** [ddns-update-method](#)

**Command changes** Version 5.4.7-0.1: command added

# ddns-update-method

**Overview** Use this command to create a new DDNS update method and enter DDNS Update Method Configuration mode.

Use the **no** variant of this command to remove a DDNS update method.

**Syntax** `ddns-update-method <method-name>`  
`no ddns-update-method <method-name>`

| Parameter                        | Description                  |
|----------------------------------|------------------------------|
| <code>&lt;method-name&gt;</code> | The name of the DDNS method. |

**Default** None

**Mode** Global Configuration

**Example** To create a method named "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)#
```

**Related commands**

`ddns enable`  
`ddns-update now`  
`debug ddns`  
`host-name (DDNS)`  
`ip ddns-update-method`  
`ipv6 ddns-update-method`  
`password (DDNS)`  
`retry-interval (DDNS)`  
`show ddns-update-method status`  
`suppress-ipv4-updates (DDNS)`  
`undebug (DDNS)`  
`update-interval (DDNS)`  
`update-url (DDNS)`  
`use-ipv4-for-ipv6-updates (DDNS)`  
`username (DDNS)`

**Command changes** Version 5.4.7-0.1: command added

# ddns-update now

**Overview** Use this command to manually update DDNS methods.

**Syntax** `ddns-update now`  
`ddns-update method <method-name> now`

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;method-name&gt;</code> | The DDNS update method name to use for the manual update. |

**Default** None

**Mode** Privileged Exec

**Usage notes** When no method name is entered, all DDNS update methods are updated. If a method name is specified, then only that method will update.

**Example** To manually update all DDNS update methods, use the command:

```
awplus# ddns-update now
```

To manually update the method "dyndns", use the command:

```
awplus# ddns-update method dyndns now
```

**Related commands** [ddns-update-method](#)

**Command changes** Version 5.4.7-0.1: command added

# debug ddns

- Overview** Use this command to enable debugging for the DDNS process.  
Use the **no** variant of this command to disable debugging for the DDNS process.
- Syntax** debug ddns  
no debug ddns
- Default** Disabled
- Mode** Privileged Exec
- Example** To enable debugging for the DDNS process, use the command:  
awplus# debug ddns  
To disable debugging for the DDNS process, use the command:  
awplus# no debug ddns
- Related commands** [ddns-update-method](#)  
[undebug \(DDNS\)](#)
- Command changes** Version 5.4.7-0.1: command added

# debug ip dns forwarding

**Overview** Use this command to enable DNS Relay debugging.  
Use the **no** variant of this command to disable DNS Relay debugging.

**Syntax** `debug ip dns forwarding`  
`no debug ip dns forwarding`

**Default** DNS Relay debugging is disabled by default.

**Mode** Privileged Exec

**Examples** To enable DNS forwarding debugging, use the commands:

```
awplus# debug ip dns forwarding
```

To disable DNS forwarding debugging, use the commands:

```
awplus# no debug ip dns forwarding
```

**Related commands** [ip dns forwarding](#)  
[show debugging ip dns forwarding](#)

# description (Domain List)

**Overview** Use this command to give a description to a domain-list.  
Use the **no** variant of this command to delete the description.

**Syntax** `description <text>`  
`no description`

| Parameter                 | Description  |
|---------------------------|--|
| <code>&lt;text&gt;</code> | Description string, 128 characters maximum. The string may contain spaces. |

**Mode** Domain List Mode

**Usage notes** When creating a domain-list, it is helpful to write a short description of what the list is to be used for.

**Examples** To add a description to a domain list, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list mydomains
awplus(config-domain-list)# description This is a useful
description of my domain list
```

To delete the description, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list mydomains
awplus(config-domain-list)# no description
```

**Related commands** [ip dns forwarding domain-list](#)

# domain (Domain List)

**Overview** Use this command to add a domain to a domain list.  
Use the **no** variant of this command to delete the domain.

**Syntax** `domain <domain-string>`  
`no domain <domain-string>`

| Parameter                          | Description  |
|------------------------------------|--|
| <code>&lt;domain-string&gt;</code> | <ul style="list-style-type: none"><li>• A domain name must only contain a-z, A-Z, 0-9, '-' (en-dash) and '.' (period) characters.</li><li>• Each sub-section of the domain must not start or end with the '-' character.</li><li>• Each sub-section must have no more than 64 characters including the '.'.</li><li>• The last section must not have a '.' at the end.</li><li>• The whole domain must be less than 254 characters long.</li></ul> |

**Mode** Domain List Mode

**Usage notes** Domain lists are objects that contain unsorted lists of domain names. After a domain list has been created, you can use this command to add domains to the domain list. There is no limit on the number of domains that can be added to a domain list.

**Examples** To add the domain "acme-solutions.com" to a domain list, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list acme-corporation
awplus(config-domain-list)# domain acme-solutions.com
```

To delete the domain, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list acme-corporation
awplus(config-domain-list)# no domain acme-solutions.com
```

**Related commands** [ip dns forwarding domain-list](#)



# host-name (DDNS)

**Overview** Use this command to add a host name for the current DDNS update method.

**NOTE:** A DDNS update method can only have one host name.

Use the **no** variant of this command to remove the host name from the current DDNS update method.

**Syntax** `host-name <host-name>`  
`no host-name`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;host-name&gt;</code> | The name of the host to be configured in conjunction with the user name and password. |

**Default** None

**Mode** DDNS Update Method Configuration

**Example** To add the host name "test.dyndns.org" for the DDNS update method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-mthod)# host-name test.dyndns.org
```

To remove the host name "test.dyndns.org" from the DDNS update method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-mthod)# no host-name
```

**Related commands** [ddns-update-method](#)

**Command changes** Version 5.4.7-0.1: command added

# ip ddns-update-method

**Overview** Use this command to enable an IPv4 interface to update DDNS with the specified DDNS update method.

Use the **no** variant of this command to disable an IPv4 interface to update DDNS with the specified DDNS update method.

**Syntax** `ip ddns-update-method <method-name>`  
`no ip ddns-update-method <method-name>`

| Parameter                        | Description                           |
|----------------------------------|---------------------------------------|
| <code>&lt;method-name&gt;</code> | A name given to a DDNS update method. |

**Default** None

**Mode** Interface Configuration

**Usage notes** A DDNS update method cannot be attached to multiple interfaces, however multiple DDNS update methods can be assigned to the same interface.

**Example** To enable IPv4 DDNS updates for a DDNS update method named “dyndns” using interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip ddns-update-method dyndns
```

To disable IPv4 DDNS updates for a DDNS update method named “dyndns” using interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip ddns-update-method dyndns
```

**Related commands** [ddns-update-method](#)

**Command changes** Version 5.4.7-0.1: command added

# ip dns forwarding

**Overview** Use this command to enable DNS Relay, the forwarding of incoming DNS queries for IP hostname-to-address translation.

Use the **no** variant of this command to disable the forwarding of incoming DNS queries for IP hostname-to-address translation.

**Syntax** `ip dns forwarding`  
`no ip dns forwarding`

**Default** The forwarding of incoming DNS query packets is disabled by default.

**Mode** Global Configuration

**Usage notes** DNS Relay is independent of the configuration of `ip domain-lookup` (which is enabled by default). If `ip domain-lookup` is disabled, but DNS Relay is enabled, the router will continue to forward DNS queries by hosts in the network to its configured name-servers.

See the `ip dns forwarding dead-time` command used with this command.

**Examples** To enable the forwarding of incoming DNS query packets, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding
```

To disable the forwarding of incoming DNS query packets, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding
```

**Related commands**

- `clear ip dns forwarding cache`
- `debug ip dns forwarding`
- `ip dns forwarding cache`
- `ip dns forwarding dead-time`
- `ip dns forwarding retry`
- `ip dns forwarding source-interface`
- `ip dns forwarding timeout`
- `ip domain-lookup`
- `ip name-server`
- `show ip dns forwarding`
- `show ip dns forwarding cache`
- `show ip dns forwarding server`

# ip dns forwarding cache

**Overview** Use this command to set the DNS Relay name resolver cache size and cache entry lifetime period. The DNS Relay name resolver cache stores the mappings between domain names and IP addresses.

Use the **no** variant of this command to set the default DNS Relay name resolver cache size and cache entry lifetime period.

Note that the lifetime period of the cache entry can be overwritten by the time-out period of the DNS reply from the DNS server if the time-out period of the DNS reply from the DNS server is smaller than the configured time-out period. The time-out period of the cache entry will only be used when the time-out period of the DNS reply from the DNS server is bigger than the time-out period configured on the device.

**Syntax** `ip dns forwarding cache [size <0-10000>] [timeout <60-3600>]`  
`no ip dns forwarding cache [size|timeout]`

| Parameter | Description   |
|-----------|---|
| <0-10000> | Number of entries in the DNS Relay name resolver cache. |
| <60-3600> | Timeout value in seconds.                               |

**Default** The default cache size is 0 (no entries) and the default lifetime is 1800 seconds.

**Mode** Global Configuration

**Examples** To set the cache size to 10 entries and the lifetime to 500 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding cache size 10 time 500
```

To set the cache size to the default, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding cache size
```

**Related commands**

- [clear ip dns forwarding cache](#)
- [debug ip dns forwarding](#)
- [ip dns forwarding](#)
- [show ip dns forwarding](#)
- [show ip dns forwarding cache](#)

**Command changes** Version 5.4.8-1.1: maximum cache limit increased to 10000

# ip dns forwarding dead-time

**Overview** Use this command to set the time period in seconds when the device stops sending any DNS requests to an unresponsive server and all retries set using [ip dns forwarding retry](#) are used. This time period is the DNS forwarding dead-time. The device stops sending DNS requests at the DNS forwarding dead-time configured and when all of the retries are used.

Use the **no** variant of this command to restore the default DNS forwarding dead-time value of 3600 seconds.

**Syntax** `ip dns forwarding dead-time <60-43200>`  
`no ip dns forwarding retry`

**Default** The default time to stop sending DNS requests to an unresponsive server is 3600 seconds.

**Mode** Global Configuration

**Usage notes** See the [ip dns forwarding retry](#) command used with this command.

**Examples** To set the DNS forwarding retry count to 50 and to set the DNS forwarding dead-time to 1800 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dead-time 1800
awplus(config)# ip dns forwarding retry 50
```

To reset the DNS retry count to the default of 2 and the DNS forwarding dead-time to the default of 3600, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dead-time
awplus(config)# no ip dns forwarding retry
```

**Related commands**

- [debug ip dns forwarding](#)
- [ip dns forwarding](#)
- [ip dns forwarding retry](#)
- [show ip dns forwarding](#)
- [show ip dns forwarding server](#)

# ip dns forwarding domain-list

**Overview** Use this command to create a domain-list that can be used as a suffix-list for DNS lookups. This command puts the device into a new mode where subsequent commands can be entered. The new mode is "Domain List Configuration" mode.

Use the **no** variant of this command to delete the domain-list.

**Syntax** `ip dns forwarding domain-list <domain-list-name>`  
`no ip dns forwarding domain-list <domain-list-name>`

| Parameter                             | Description       |
|---------------------------------------|-------------------|
| <code>&lt;domain-list-name&gt;</code> | Name of the list. |

**Mode** Global Configuration

**Usage notes** The domain list can be used by features that need to match against domains. A domain list by itself does nothing; it must be attached to another feature to have functionality (like a prefix-list). For example, the domain list can be used as a suffix list on an DNS name-server. The DNS server can be either statically configured, or learned over a PPP connection.

Note that this command is separate from the **ip domain-list** command, which is used by DNS client to append a domain on to the end of a partial hostname to form a fully-qualified domain.

**Examples** To create a domain list to include domains that are internal to the company such as "engineering.acme" or "intranet.acme", use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list corporatedomains
awplus(config-domain-list)# description internal network domain
awplus(config-domain-list)# domain engineering.acme
awplus(config-domain-list)# domain intranet.acme
```

To delete the domain list, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding domain-list
corporatedomains
```

**Related commands** [description \(Domain List\)](#)  
[domain \(Domain List\)](#)

# ip dns forwarding retry

**Overview** Use this command to set the number of times DNS Relay will retry to forward DNS queries. The device stops sending DNS requests to an unresponsive server at the time set using the [ip dns forwarding dead-time](#) command and when all of the retries are used.

Use the **no** variant of this command to set the number of retries to the default of 2.

**Syntax** `ip dns forwarding retry <0-100>`  
`no ip dns forwarding retry`

**Default** The default number of retries is 2 DNS requests to an unresponsive server.

**Mode** Global Configuration

**Usage notes** See the [ip dns forwarding dead-time](#) command used with this command.

**Examples** To set the DNS forwarding retry count to 50 and to set the DNS forwarding dead-time to 1800 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding retry 50
awplus(config)# ip dns forwarding dead-time 1800
```

To reset the DNS retry count to the default of 2 and the DNS forwarding dead-time to the default of 3600 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding retry
awplus(config)# no ip dns forwarding dead-time
```

**Related commands**

- [debug ip dns forwarding](#)
- [ip dns forwarding](#)
- [ip dns forwarding dead-time](#)
- [show ip dns forwarding](#)

# ip dns forwarding source-interface

**Overview** Use this command to set the interface to use for forwarding and receiving DNS queries.

Use the **no** variant of this command to unset the interface used for forwarding and receiving DNS queries.

**Syntax** `ip dns forwarding source-interface <interface-name>`  
`no ip dns forwarding source-interface`

**Default** The default is that no interface is set and the device selects the appropriate source IP address automatically.

**Mode** Global Configuration

**Examples** To set `vlan1` as the source interface for relayed DNS queries, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding source-interface vlan1
```

To clear the source interface for relayed DNS queries, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding source-interface
```

**Related commands** [debug ip dns forwarding](#)  
[ip dns forwarding](#)  
[show ip dns forwarding](#)



# ip dns forwarding timeout

**Overview** Use this command to set the time period for the DNS Relay to wait for a DNS response.

Use the **no** variant of this command to set the time period to wait for a DNS response to the default of 3 seconds.

**Syntax** `ip dns forwarding timeout <0-3600>`  
`no ip dns forwarding timeout`

**Default** The default timeout value is 3 seconds.

**Mode** Global Configuration

**Examples** To set the timeout value to 12 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding timeout 12
```

To set the timeout value to the default of 3 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding timeout
```

**Related commands** [debug ip dns forwarding](#)  
[ip dns forwarding](#)  
[show ip dns forwarding](#)

# ip domain-list

**Overview** This command adds a domain to the DNS list. Domains are appended to incomplete host names in DNS requests. Each domain in this list is tried in turn in DNS lookups. This list is ordered so that the first entry you create is checked first.

The **no** variant of this command deletes a domain from the list.

**Syntax** `ip domain-list <domain-name>`  
`no ip domain-list <domain-name>`

| Parameter                        | Description                               |
|----------------------------------|---|
| <code>&lt;domain-name&gt;</code> | Domain string, for example "company.com". |

**Mode** Global Configuration

**Usage notes** If there are no domains in the DNS list, then your device uses the domain specified with the `ip domain-name` command. If any domain exists in the DNS list, then the device does not use the domain set using the **ip domain-name** command.

**Example** To add the domain `example.net` to the DNS list, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-list example.net
```

**Related commands** `ip domain-lookup`  
`ip domain-name`  
`show ip domain-list`

# ip domain-lookup

**Overview** This command enables the DNS client on your device. This allows you to use domain names instead of IP addresses in commands. The DNS client resolves the domain name into an IP address by sending a DNS inquiry to a DNS server, specified with the `ip name-server` command.

It is possible to configure the DNS client to use the DNS relay to resolve domain lookups originating from the device itself. This configuration may be preferred, as the DNS relay provides additional functionality that is not available in the DNS client, such as caching, a configurable timeout length, and other options.

The **no** variant of this command disables the DNS client. The client will not attempt to resolve domain names. You must use IP addresses to specify hosts in commands.

**Syntax** `ip domain-lookup [via-relay]`  
`no ip domain-lookup`

| Parameter              | Description                      |
|------------------------|----------------------------------|
| <code>via-relay</code> | Perform resolution via DNS relay |

**Mode** Global Configuration

**Usage notes** The client is enabled by default. However, it does not attempt DNS inquiries unless there is a DNS server configured.

**Examples** To enable the DNS client on your device, use the following commands:

```
awplus# configure terminal  
awplus(config)# ip domain-lookup
```

To configure the DNS client to perform resolution via the DNS relay, use the following commands:

```
awplus# configure terminal  
awplus(config)# ip domain-lookup via-relay  
awplus(config)# ip dns forwarding
```

To disable the DNS client on your device, use the following commands:

```
awplus# configure terminal  
awplus(config)# no ip domain-lookup
```

**Related commands**

- ip domain-list
- ip domain-name
- ip name-server
- show hosts
- show ip name-server

**Command changes** Version 5.4.8-1.1: via-relay parameter added

# ip domain-name

**Overview** This command sets a default domain for the DNS. The DNS client appends this domain to incomplete host-names in DNS requests.

The **no** variant of this command removes the domain-name previously set by this command.

**Syntax** `ip domain-name <domain-name>`  
`no ip domain-name <domain-name>`

**Mode** Global Configuration

**Usage notes** If there are no domains in the DNS list (created using the [ip domain-list](#) command) then your device uses the domain specified with this command. If any domain exists in the DNS list, then the device does not use the domain configured with this command.

When your device is using its DHCP client for an interface, it can receive Option 15 from the DHCP server. This option replaces the domain name set with this command.

**Example** To configure the domain name, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-name company.com
```

**Related commands** [ip domain-list](#)  
[show ip domain-list](#)  
[show ip domain-name](#)

# ip name-server

**Overview** Use this command to add IPv4 or IPv6 DNS server addresses. The DNS client on your device sends DNS queries to IP addresses in this list when trying to resolve a host name. Host names cannot be resolved until you have added at least one server to this list. A maximum of three name servers can be added to this list.

The **no** variant of this command removes the specified DNS name-server address.

**Syntax** `ip name-server <ip-addr> [suffix-list <domain-list>]`  
`no ip name-server <ip-addr> [suffix-list]`

| Parameter                        | Description  |
|----------------------------------|--|
| <code>&lt;ip-addr&gt;</code>     | The IP address of the DNS server that is being added to the name server list. The address is entered in the form A.B.C.D for an IPv4 address, or in the form X:X::X:X for an IPv6 address. The order that you enter the servers in, is the order in which they will be used. |
| <code>suffix-list</code>         | Specify domain suffixes that should be directed to this name server  |
| <code>&lt;domain-list&gt;</code> | The name of the DNS domain-list  |

**Mode** Global Configuration

**Usage notes** To allow the device to operate as a DNS proxy, your device must have learned about a DNS name-server to forward requests to. Name-servers can be learned through the following means:

- Manual configuration, using the **ip name-server** command
- Learned from DHCP server with Option 6
- Learned over a PPP tunnel if the neighbor advertises the DNS server

Use this command to statically configure a DNS name-server for the device to use.

The order that you enter the servers in, is the order in which they will be used.

For more information about PPP and DNS, see the [PPP Feature Overview and Configuration Guide](#).

**Examples** To allow a device to send DNS queries to a DNS server with the IPv4 address 10.10.10.5, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server 10.10.10.5
```

To enable your device to send DNS queries to a DNS server with the IPv6 address 2001:0db8:010d::1, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server 2001:0db8:010d::1
```

For DNS relay, to direct DNS lookups for domains with suffixes of "engineering.acme" or "intranet.acme" to an internal corporate name-server, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list corporatedomains
awplus(config-domain-list)# description Our internal network
domains; do not send DNS requests to internet
awplus(config-domain-list)# domain engineering.acme
awplus(config-domain-list)# domain intranet.acme
awplus(config-domain-list)# exit
awplus(config)# ip name-server 172.16.0.1 suffix-list
corporatedomains
```

**Related  
commands**

[ip domain-list](#)  
[ip domain-lookup](#)  
[ip domain-name](#)  
[show ip dns forwarding cache](#)  
[show ip name-server](#)

**Command  
changes**

Version 5.4.6-2.1: VRF-lite support added to AR-series devices.

# ip name-server preferred-order

**Overview** Use this command to choose between using statically-configured DNS servers or dynamically-learned DNS servers.

Use the **no** variant of this command to set the DNS servers back to the default setting of dynamic.

**Syntax** `ip name-server preferred-order {dynamic|static}`  
`no ip name-server preferred-order`

| Parameter | Description                                  |
|-----------|--|
| dynamic   | Use dynamically learned DNS servers first.   |
| static    | Use statically configured DNS servers first. |

**Default** dynamic

**Mode** Global Configuration

**Usage notes** This command is used to choose which DNS server set to use first. Select either the **dynamic** or **static** parameter.

**Examples** To configure the preference to use static servers first, use the commands:

```
awplus# configure terminal  
awplus(config)# ip name-server preferred-order static
```

To configure the preference to use dynamically-learned servers first, use the commands:

```
awplus# configure terminal  
awplus(config)# ip name-server preferred-order dynamic
```

or

```
awplus# configure terminal  
awplus(config)# no ip name-server preferred-order
```

**Related commands** [ip address dhcp](#)  
[ip name-server](#)  
[ipv6 address dhcp](#)  
[ppp ipcp dns](#)  
[show ip name-server](#)

**Command changes** Version 5.4.9-0.1: command added



# ipv6 ddns-update-method

**Overview** Use this command to enable an IPv6 interface to update DDNS with the specified DDNS update method.

Use the **no** variant of this command to disable an IPv6 interface to update DDNS with the specified DDNS update method.

**Syntax** `ipv6 ddns-update-method <method-name>`  
`no ipv6 ddns-update-method <method-name>`

| Parameter                        | Description                           |
|----------------------------------|---------------------------------------|
| <code>&lt;method-name&gt;</code> | A name given to a DDNS update method. |

**Default** None

**Mode** Interface Configuration

**Usage notes** A DDNS update method cannot be attached to multiple interfaces, however multiple DDNS update methods can be assigned to the same interface.

**Example** To enable IPv6 DDNS updates for a DDNS update method named "dyndns" using interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ddns-update-method dyndns
```

To disable IPv6 DDNS updates for a DDNS update method named "dyndns" using interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 ddns-update-method dyndns
```

**Related commands** [ddns-update-method](#)

**Command changes** Version 5.4.7-0.1: command added

# password (DDNS)

**Overview** Use this command to add a password to the current DDNS update method.  
Use the **no** variant of this command to remove a password from the current DDNS update method.

**Syntax** password <password>  
no password

| Parameter  | Description  |
|------------|--|
| <password> | The password to be configured in conjunction with the user name and host name. |

**Default** None

**Mode** DDNS Update Method Configuration

**Example** To configure the password "test" for the method "dyndns", use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-mthod)# password test
```

To remove the password "test" from the method "dyndns", use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-mthod)# no password
```

**Related commands** [ddns-update-method](#)

**Command changes** Version 5.4.7-0.1: command added

# ppp ipcp dns

**Overview** Use this command to configure the primary and secondary DNS (Domain Name System) IP addresses for IPCP (Internet Protocol Control Protocol) on a given PPP interface.

Use the **no** variant of this command to remove the primary and secondary DNS IP addresses for IPCP on a given PPP interface, and remove any optional parameters configured for DNS.

**Syntax** `ppp ipcp dns [<primary> [<secondary>]][required|reject|request]`  
`no ppp ipcp dns`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;primary&gt;</code>   | Specify the primary DNS address for a given PPP interface to the peer.    |
| <code>&lt;secondary&gt;</code> | Specify the secondary DNS address for a given PPP interface to the peer.  |
| <code>required</code>          | Request DNS addresses from the peer, and close the link if none is given. |
| <code>reject</code>            | Reject negotiations with the peer (default).                              |
| <code>request</code>           | Request DNS addresses from the peer.                                      |

**Default** By default no IPCP DNS server request is sent to the peer.

**Mode** Interface Configuration

**Usage notes** Use the optional parameters to configure PPP IPCP DNS options for accepting, rejecting or requesting DNS addresses from the peer. Use the optional primary and secondary or primary only DNS server address placeholders to specify DNS server addresses to the peer.

The no variant of this command also stops IPCP DNS request messages being sent to the peer.

**Examples** To configure the PPP interface `ppp0` to require a DNS IP address from the peer, and close the link if a DNS IP address is not given, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns required
```

To configure the PPP interface `ppp0` to require a DNS IP address from the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns request
```

To configure the PPP interface `ppp0` to reject a DNS IP address from the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns reject
```

To configure the PPP interface `ppp0` to supply primary and secondary DNS server addresses to the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns 10.1.1.2 10.1.1.3
```

To configure the PPP interface `ppp0` to supply a primary but not a secondary DNS server address to the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns 10.1.1.2
```

**Related  
commands**

[ip address negotiated](#)  
[peer default ip address](#)  
[peer neighbor-route](#)  
[show running-config interface](#)

# ppp ipcp dns suffix-list

**Overview** Use this command to configure a suffix-list to be associated with DNS name-servers learned over the PPP connection.

Use the **no** variant of this command to remove the suffix-list.

**Syntax** `ppp ipcp dns suffix-list <domain-list-name>`  
`no ppp ipcp dns suffix-list`

| Parameter                             | Description                     |
|---------------------------------------|---------------------------------|
| <code>&lt;domain-list-name&gt;</code> | The name of the DNS domain-list |

**Mode** Interface Configuration

**Usage notes** A PPP connection can be configured to learn DNS servers from the remote peer by using the command `ppp ipcp dns` command.

This command allows a user to associate a domain-list to be used to match against the suffixes of incoming DNS requests. For example, a customer branch office may have a router that is used to give remote-access to their head office, over which they learn the IP address of the head office's DNS server. A domain list can be created that contains a suffix used for services internal to that company, for example, "example.lc". This domain-list is associated as a suffix-list to the PPP connection. So when the PPP connection is completed with the head office, users at the branch office that browse to "intranet.example.lc" will have the DNS request forwarded to the DNS server learned over the PPP connection. Without having the suffix-list configured, the DNS request for "intranet.example.lc" would instead be sent to the primary DNS server, which is likely to be the branch office's ISP, and they will simply respond with a negative reply, because .example.lc is not a globally routable domain.

**Examples** At a branch office, to direct DNS lookups for domains with suffixes of "engineering.acme" or "intranet.acme" to an internal corporate name-server run at head-office that was learned over a PPP connection, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list corporatedomains
host(config-domain-list)# description Our internal network
domains; do not send DNS requests to internet
host(config-domain-list)# domain engineering.acme
host(config-domain-list)# domain intranet.acme
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns required
awplus(config-if)# ppp ipcp dns suffix-list corporatedomains
```

**Related  
commands** [ip dns forwarding domain-list](#)  
[ppp ipcp dns](#)

# retry-interval (DDNS)

**Overview** Use this command to enable DDNS update retries. Retries are attempted after a DDNS update fails after the specified interval. If the DDNS update keeps failing, then no more than the specified maximum retries are attempted.

**NOTE:** *The retry interval is used for one DDNS update at one time, so if an update is not complete within the specified interval, an update will not begin until it has completed.*

Use the **no** variant of this command to disable DDNS update retries.

**Syntax** `retry-interval <1-3888000> maximum-retries <1-100>`  
`no retry-interval`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;1-3888000&gt;</code> | The retry interval in seconds (from 1 second to 4.5 days), after which a failed DDNS update will be retried. |
| <code>&lt;1-100&gt;</code>     | The maximum number of times a retry is allowed.  |

**Default** Disabled

**Mode** DDNS Update Method Configuration

**Usage notes** If an update is triggered by another source, such as an IP address change or a manual update, then the retry counter will start again from the beginning.

**Example** To enable DDNS update retry attempts every hour up to 5 times for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# retry-interval 3600
maximum-retries 5
```

To disable DDNS update retry attempts for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# no retry-interval
```

**Related commands** [ddns-update-method](#)

**Command changes** Version 5.4.7-0.1: command added

# show ddns-update-method status

**Overview** Use this command to show the status of the configured DDNS update methods.

**Syntax** show ddns-update-method status

**Mode** User Exec and Privileged Exec

**Example** To display the status of DDNS update methods currently configured on your device, use the command:

```
awplus# show ddns-update-method status
```

**Output** Figure 15-1: Example output from **show ddns-update-method status**

```
awplus#show ddns-update-method status

Dynamic DNS updates are enabled

-----
Update Method Name      test
Hostname                 test.dnsalias.org
IPv4 Interface          vlan1
IPv4 Address             192.168.10.100
IPv4 Status              Update succeeded
IPv4 Update Result      good 192.168.10.100
IPv6 Interface          vlan1
IPv6 Address             333::f195
IPv6 Status              Update succeeded
IPv6 Update Result      good 0333:0000:0000:0000:0000:0000:0000:f195
Last update              Last update Aug 25, 2019 06:54:24
```

**Related commands** [ddns-update-method](#)

**Command changes** Version 5.4.7-0.1: command added



# show debugging ip dns forwarding

**Overview** Use this command to see what debugging is turned on for DNS Relay. DNS Relay debugging is set using the **debug ip dns forwarding** command.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show debugging ip dns forwarding`

**Mode** User Exec and Privileged Exec

**Example** To display the DNS Relay debugging status, use the command:

```
awplus# show debugging ip dns forwarding
```

**Output** Figure 15-2: Example output from the **show debugging ip dns forwarding** command

```
awplus#show debugging ip dns forwarding

DNS Relay debugging status:
debugging is on
```

**Related commands** [debug ip dns forwarding](#)

# show hosts

**Overview** This command shows the default domain, domain list, and name servers configured on your device.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show hosts

**Mode** User Exec and Privileged Exec

**Example** To display the default domain, use the command:

```
awplus# show hosts
```

**Output** Figure 15-3: Example output from the **show hosts** command when **no ip domain-lookup** is configured

```
awplus#show hosts

Default domain is not set
Name/address lookup is disabled
```

Figure 15-4: Example output from the **show hosts** command when **ip domain-lookup** is configured

```
awplus#show hosts

Default domain is mycompany.com
Domain list: company.com
Name/address lookup uses domain service
Name servers are 10.10.0.2 10.10.0.88
```

Figure 15-5: Example output from the **show hosts** command when **ip domain-lookup via-relay** is configured

```
awplus#show hosts

Default domain is mycompany.com
Domain list: company.com
Name/address lookup uses domain relay service
Name servers are 10.10.0.2 10.10.0.88
```

**Related commands**

- [ip domain-list](#)
- [ip domain-lookup](#)
- [ip domain-name](#)
- [ip name-server](#)

# show ip dns forwarding

**Overview** Use this command to display the DNS Relay status.

**Syntax** `show ip dns forwarding`

**Mode** User Exec and Privileged Exec

**Examples** To display the DNS Relay status, use the command:

```
awplus# show ip dns forwarding
```

**Output** Figure 15-6: 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 15-7: Example output from the **show ip dns forwarding cache** command

```
awplus#show ip dns forwarding cache
IPv4 addresses in cache:    3
IPv6 addresses in cache:    0
Cache size: 1000
Host                        Address                Expires  Flags
www.example.com            172.16.1.1.            180
mail.example.com           www.example.com         180 CNAME
www.example.com            172.16.1.1.            180 REVERSE
mail.example.com           172.16.1.5.            180
```

**Related commands** [ip dns forwarding cache](#)  
[ip name-server](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.  
Version 5.4.8-1.1: additional cache counters added to output.

# show ip dns forwarding server

**Overview** Use this command to display the status of DNS forwarding name servers.

**Syntax** `show ip dns forwarding server`

| Parameter         | Description  |
|-------------------|--|
| forwarding server | Display information about the DNS forwarding name servers. |

**Mode** User Exec and Privileged Exec

**Examples** To display the status of DNS Relay name servers, use the command:

```
awplus# show ip dns forwarding server
```

**Output** Figure 15-8: Example output from the **show ip dns forwarding server** command

```
awplus#show ip dns forwarding server
```

| Servers    | Forwards | Fails | Dead-Time |
|------------|----------|-------|-----------|
| 172.16.1.1 | 12       | 0     | active    |
| 172.16.1.2 | 6        | 3     | 3900      |

**Related commands** [ip dns forwarding](#)

[ip dns forwarding dead-time](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# show ip domain-list

**Overview** This command shows the domains configured in the domain list. The DNS client uses the domains in this list to append incomplete hostnames when sending a DNS inquiry to a DNS server.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip domain-list`

**Mode** User Exec and Privileged Exec

**Example** To display the list of domains in the domain list, use the command:

```
awplus# show ip domain-list
```

**Output** Figure 15-9: Example output from the **show ip domain-list** command

```
awplus#show ip domain-list
alliedtelesis.com
mycompany.com
```

**Related commands** [ip domain-list](#)  
[ip domain-lookup](#)

# show ip domain-name

**Overview** This command shows the default domain configured on your device. When there are no entries in the DNS list, the DNS client appends this domain to incomplete hostnames when sending a DNS inquiry to a DNS server.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip domain-name`

**Mode** User Exec and Privileged Exec

**Example** To display the default domain configured on your device, use the command:

```
awplus# show ip domain-name
```

**Output** Figure 15-10: Example output from the **show ip domain-name** command

```
awplus#show ip domain-name  
alliedtelesis.com
```

**Related commands** [ip domain-name](#)  
[ip domain-lookup](#)

# show ip name-server

**Overview** This command displays a list of IPv4 and IPv6 DNS server addresses that your device will send DNS requests to. This is a static list configured using the `ip name-server` command.

The command will also show any domain-list that has been associated as suffix-list with the DNS server, and the domains that will be preferentially directed to that DNS server.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip name-server`

**Mode** User Exec and Privileged Exec

**Example** To display the list of DNS servers that your device sends DNS requests to, use the command:

```
awplus# show ip name-server
```

**Output** Figure 15-11: 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
```

**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 15-12: Example output from the **show ip name-server** command

```
awplus#show ip name-server
Currently learned name-servers
10.36.200.165 dynamic (ppp0)
10.35.12.20 dynamic (ppp1), using suffix-list mysuffixlist:
    test.com
    intranet.interslice.com
10.37.84.97 static
130.37.84.97 static
```

**Related commands** [ip domain-lookup](#)  
[ip name-server](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.



# suppress-ipv4-updates (DDNS)

**Overview** Use this command to suppress IPv4 updates from being sent.  
Use the **no** variant of this command to stop suppressing IPv4 updates from being sent.

**Syntax** `suppress-ipv4-updates`  
`no suppress-ipv4-updates`

**Default** Disabled

**Mode** DDNS Update Method Configuration

**Usage notes** This command is used in conjunction with the **use-ipv4-for-ipv6-updates** command. IPv4 DDNS updates are suppressed so that only IPv6 updates are sent.

**NOTE:** *The IPv4 DNS entry may be updated using the source IPv4 address used.*

**Example** To suppress IPv4 updates and send IPv6 updates instead for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method-dyndns
awplus(config-ddns-update-method)# use-ipv4-for-ipv6-updates
awplus(config-ddns-update-method)# suppress-ipv4-updates
```

**Related commands** [ddns-update-method](#)  
[use-ipv4-for-ipv6-updates \(DDNS\)](#)

**Command changes** Version 5.4.7-0.1: command added

# undebug (DDNS)

**Overview** Use this command to disable debugging for the DDNS process.

**Syntax** `undebug ddns`

**Default** Disabled

**Mode** Privileged Exec

**Example** To disable debugging for the DDNS process, use the command:

```
awplus# undebug ddns
```

**Related commands** [ddns-update-method](#)  
[debug ddns](#)

**Command changes** Version 5.4.7-0.1: command added

# update-interval (DDNS)

**Overview** Use this command to specify the time interval between periodic DDNS updates. Use the **no** variant of this command to disable periodic DDNS updates.

**Syntax** `update-interval <1-64800>`  
`no update-interval`

| Parameter                    | Description   |
|------------------------------|---|
| <code>&lt;1-64800&gt;</code> | Update interval time in minutes (from 1 minute to 45 days). |

**Default** Disabled

**Mode** DDNS Update Method Configuration

**Examples** To enable periodic DDNS updates every day for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# update-interval 1440
```

To enable periodic DDNS updates every 28 days for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# update-interval 40320
```

To disable periodic DDNS updates for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# no update-interval
```

**Related commands** [ddns-update-method](#)

**Command changes** Version 5.4.7-0.1: command added

# update-url (DDNS)

**Overview** Use this command to configure a URL for DDNS updates for the current DDNS update method.

Use the **no** variant of this command to remove an update URL from a DDNS update method.

**Syntax** `update-url <url-name>`  
`no update-url <url-name>`

| Parameter                     | Description  |
|-------------------------------|--|
| <code>&lt;url-name&gt;</code> | The update URL is provided by the DDNS provider and can be configured with the following placeholder tokens: <ul style="list-style-type: none"><li>• <code>&lt;USERNAME&gt;</code></li><li>• <code>&lt;PASSWORD&gt;</code></li><li>• <code>&lt;HOST-NAME&gt;</code></li><li>• <code>&lt;IPADDRESS&gt;</code></li></ul> To specify the values for <code>&lt;USERNAME&gt;</code> , <code>&lt;PASSWORD&gt;</code> and <code>&lt;HOST-NAME&gt;</code> , use the commands <b>username</b> , <b>password</b> and <b>hostname</b> . The value for <code>&lt;IPADDRESS&gt;</code> is populated automatically from the interface IP settings. |

**Default** None

**Mode** DDNS Update Method Configuration

**Usage notes** The update URL (provided by the DDNS provider) can include a user name, password, host name and/or IP address. These user values are optional because they may vary depending on the DDNS provider's update URLs. AlliedWare Plus requires you to enter the required parameters for the update URL using the following placeholder tokens:

- for the user name enter "`<USERNAME>`"
- for the password enter "`<PASSWORD>`"
- for the host name enter "`<HOST-NAME>`"
- for the IP address enter "`<IPADDRESS>`"

For example, for DynDNS the following update URL can be used:

```
http://username:password@members.dyndns.org/nic/update?  
SYSTEM=dyndns&hostname=<h>&myip=<a>
```

To configure this URL, use the following command including the placeholder tokens as written here:

```
awplus(config-ddns-update-method)# update-url  
http://<USERNAME>:<PASSWORD>@members.dyndns.org/nic/update?  
SYSTEM=dyndns&hostname=<HOST-NAME>&myip=<IPADDRESS>
```

DynDNS also has the following update URL that can be used instead:

```
http://<USERNAME>:<PASSWORD>@members.dyndns.org/v3/update?  
hostname=<HOST-NAME>&myip=<IPADDRESS>
```

**NOTE:** URLs that contain the character "?" activate help from the command line. To stop the help from activating enter the "?" in the command line, then press Ctrl+v.

For more information and examples, see the [Domain Name System \(DNS\) for AlliedWare Plus AR-Series Firewalls Feature Overview and Configuration Guide](#).

**Examples** To use members.dyndns.org/nic/update as the update URL for the provider DynDNS, with the method called "dyndns" that uses HTTP, use the following commands:

```
awplus# configure terminal  
awplus(config)# ddns-update-method dyndns  
awplus(config-ddns-update-method)# update-url  
http://<USERNAME>:<PASSWORD>@members.dyndns.org/nic/update?  
SYSTEM=dyndns&hostname=<HOST-NAME>&myip=<IPADDRESS>
```

To use members.dyndns.org/v3/update as the update URL for the provider DynDNS, with the method called "dyndns" that uses HTTP, use the following commands:

```
awplus# configure terminal  
awplus(config)# ddns-update-method dyndns  
awplus(config-ddns-update-method)# update-url  
http://<USERNAME>:<PASSWORD>@members.dyndns.org/v3/update?  
hostname=<HOST-NAME>&myip=<IPADDRESS>
```

To use members.dyndns.org/v3/update as the update URL for the provider DynDNS, with the method called "dyndns" that uses HTTPS/SSL, use the following commands:

```
awplus# configure terminal  
awplus(config)# ddns-update-method dyndns  
awplus(config-ddns-update-method)# update-url  
https://<USERNAME>:<PASSWORD>@members.dyndns.org/v3/update?  
hostname=<HOST-NAME>&myip=<IPADDRESS>
```

To use members.dyndns.org/v3/update as the update URL for the provider DynDNS, with the method called "dyndns" that uses HTTP on port 8245, use the following commands:

```
awplus# configure terminal  
awplus(config)# ddns-update-method dyndns  
awplus(config-ddns-update-method)# update-url  
http://<USERNAME>:<PASSWORD>@members.dyndns.org:8245/v3/  
update?hostname=<HOST-NAME>&myip=<IPADDRESS>
```

To remove the update URL from the method called “dyndns”, use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# no update-url
```

**Related commands** [ddns-update-method](#)

**Command changes** Version 5.4.7-0.1: command added

# use-ipv4-for-ipv6-updates (DDNS)

**Overview** Use this command to send IPv6 updates using IPv4.  
Use the **no** variant of this command to stop sending IPv6 updates using IPv4.

**Syntax** `use-ipv4-for-ipv6-updates`  
`no use-ipv4-for-ipv6-updates`

**Default** Disabled

**Mode** DDNS Update Method Configuration

**Usage notes** If your DDNS provider supports IPv6 but does not support sending updates in IPv6 then this command is used so IPv6 updates can be sent using IPv4 instead. The **suppress-ipv4-updates** command is used in conjunction with this command to suppress IPv4 updates and send only IPv6 updates instead.

**example** To send IPv6 updates using IPv4 for the method "dyndns" and to suppress IPv4 updates, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# use-ipv4-for-ipv6-updates
awplus(config-ddns-update-method)# suppress-ipv4-updates
```

**Related commands** [ddns-update-method](#)  
[suppress-ipv4-updates \(DDNS\)](#)

**Command changes** Version 5.4.7-0.1: command added

# username (DDNS)

**Overview** Use this command to add a user name to the current DDNS update method.  
Use the **no** variant of this command to remove a user name from the current DDNS update method.

**Syntax** `username <user-name>`  
`no username`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;user-name&gt;</code> | The name of the user to be configured in conjunction with the password and host name. |

**Default** None

**Mode** DDNS Update Method Configuration

**Example** To configure the username "atlnz" for the method "dyndns", use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-mthod)# username atlnz
```

To remove the username "atlnz" from the method "dyndns", use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-mthod)# no username
```

**Related commands** [ddns-update-method](#)

**Command changes** Version 5.4.7-0.1: command added



# 16

# IPv6 Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure IPv6. For more information, see the [IPv6 Feature Overview and Configuration Guide](#).

- Command List**
- “clear ipv6 neighbors” on page 571
  - “ipv6 address” on page 572
  - “ipv6 address autoconfig” on page 574
  - “ipv6 address suffix” on page 576
  - “ipv6 enable” on page 577
  - “ipv6 eui64-linklocal” on page 579
  - “ipv6 forwarding” on page 580
  - “ipv6 nd accept-ra-pinfo” on page 581
  - “ipv6 nd current-hoplimit” on page 582
  - “ipv6 nd managed-config-flag” on page 584
  - “ipv6 nd minimum-ra-interval” on page 585
  - “ipv6 nd other-config-flag” on page 587
  - “ipv6 nd prefix” on page 588
  - “ipv6 nd proxy interface” on page 590
  - “ipv6 nd ra-interval” on page 591
  - “ipv6 nd ra-lifetime” on page 592
  - “ipv6 nd reachable-time” on page 593
  - “ipv6 nd retransmission-time” on page 595
  - “ipv6 nd suppress-ra” on page 597

- [“ipv6 neighbor”](#) on page 598
- [“ipv6 opportunistic-nd”](#) on page 599
- [“ipv6 route”](#) on page 600
- [“ipv6 unreachable”](#) on page 601
- [“optimistic-nd”](#) on page 602
- [“ping ipv6”](#) on page 603
- [“show ipv6 forwarding”](#) on page 605
- [“show ipv6 interface brief”](#) on page 606
- [“show ipv6 neighbors”](#) on page 607
- [“show ipv6 route”](#) on page 608
- [“show ipv6 route summary”](#) on page 609
- [“traceroute ipv6”](#) on page 610

# clear ipv6 neighbors

**Overview** Use this command to clear all dynamic IPv6 neighbor entries.

**Syntax** `clear ipv6 neighbors`

**Mode** Privileged Exec

**Example** `awplus# clear ipv6 neighbors`

# ipv6 address

**Overview** Use this command to set the IPv6 address of an interface. The command also enables IPv6 on the interface, which creates an EUI-64 link-local address as well as enabling RA processing and SLAAC.

To stop the device from processing prefix information (routes and addresses from the received Router Advertisements) use the command **no ipv6 nd accept-ra-pinfo**.

To remove the EUI-64 link-local address, use the command **no ipv6 eui64-linklocal**.

Use the **no** variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

**Syntax** `ipv6 address <ipv6-addr/prefix-length>`  
`no ipv6 address <ipv6-addr/prefix-length>`

| Parameter                                    | Description   |
|--|---|
| <code>&lt;ipv6-addr/prefix-length&gt;</code> | Specifies the IPv6 address to be set. The IPv6 address uses the format X:X::X/Prefix-Length. The prefix-length is usually set between 0 and 64. |

**Mode** Interface Configuration for a VLAN interface, a PPP interface, or a tunnel.

**Usage notes** 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 vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the VLAN interface vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

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 assign the IPv6 address to the tunnel tunnel0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
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
```

**Related  
commands**

- [ipv6 address autoconfig](#)
- [ipv6 address dhcp](#)
- [ipv6 dhcp server](#)
- [ipv6 enable](#)
- [ipv6 eui64-linklocal](#)
- [show running-config](#)
- [show ipv6 interface brief](#)
- [show ipv6 route](#)

# ipv6 address autoconfig

**Overview** Use this command to enable IPv6 stateless address autoconfiguration (SLAAC) for an interface. This configures an IPv6 address on an interface derived from the MAC address on the interface.

Use the **no** variant of this command to disable IPv6 SLAAC on an interface. Note that if no global addresses are left after removing all IPv6 autoconfigured addresses then IPv6 is disabled.

**Syntax** `ipv6 address autoconfig`  
`no ipv6 address autoconfig`

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** Use this command to enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6.

IPv6 hosts can configure themselves when connected to an IPv6 network using ICMPv6 (Internet Control Message Protocol version 6) router discovery messages. Configured routers respond with a Router Advertisement (RA) containing configuration parameters for IPv6 hosts.

The SLAAC process derives the interface identifier of the IPv6 address from the MAC address of the interface. When applying SLAAC to an interface, note that the MAC address of the default VLAN is applied to the interface if the interface does not have its own MAC address.

If SLAAC is not suitable then a network can use stateful configuration with DHCPv6 (Dynamic Host Configuration Protocol version 6) Relay, or hosts can be configured statically. See [ip dhcp-relay server-address](#) for the DHCPv6 Relay server command description and examples. See the [IP Feature Overview and Configuration Guide](#) for more information about DNS Relay.

Note that 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 ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 address autoconfig
```

To disable SLAAC on ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 address autoconfig
```

**Related  
commands**

[ipv6 address](#)  
[ipv6 enable](#)  
[show ipv6 interface brief](#)  
[show running-config](#)

# ipv6 address suffix

**Overview** Use this command to configure the suffix to use when generating an address from prefix information. Any addresses that were created with the EUI-64 suffix will be removed, and new addresses will be added after the next Router Advertisement.

Use the **no** variant of this command to set it back to the default of disabled or set to `::` for the same result as the **no** variant.

**Syntax** `ipv6 address suffix <ipv6-addr-suffix>`  
`no ipv6 address suffix`

| Parameter                             | Description  |
|---------------------------------------|--|
| <code>&lt;ipv6-addr-suffix&gt;</code> | In the format of <code>::X:X:X</code> , for example <code>::a2d8:0fd8</code> |

**Default** Disabled

**Mode** Interface Configuration

**Example** To configure the suffix to use when generating an address from prefix information on eth1, use the command:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 address suffix ::a2d8:0fd8
```

**Related commands** [ipv6 nd accept-ra-pinfo](#)  
[show running-config interface](#)

**Command changes** Version 5.4.8-2.1: command added



# ipv6 enable

**Overview** Use this command to enable automatic configuration of a link-local IPv6 address on an interface using Stateless Automatic Address Configuration (SLAAC). By default, the EUI-64 method is used to generate the link-local address.

Use the **no** variant of this command to disable IPv6 on an interface without a global address. Note, to stop EUI-64 from generating the automatic link-local address, use the command **no ipv6 eui64-linklocal**.

**Syntax** `ipv6 enable`  
`no ipv6 enable`

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** The **ipv6 enable** command automatically configures an IPv6 link-local address on the interface and enables the interface for IPv6 processing.

A link-local address is an IP (Internet Protocol) address that is only used for communications in the local network, or for a point-to-point connection. Routing does not forward packets with link-local addresses. IPv6 requires that a link-local address is assigned to each interface that has the IPv6 protocol enabled, and when addresses are assigned to interfaces for routing IPv6 packets.

Note that 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.

**Default** All interfaces default to IPv6-down with no address.

**Examples** To enable IPv6 with only a link-local IPv6 address on the VLAN interface vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 enable
```

To disable IPv6 with only a link-local IPv6 address on the VLAN interface vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 enable
```

To enable IPv6 with only a link-local IPv6 address on the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 enable
```

To disable IPv6 with only a link-local IPv6 address on the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 enable
```

**Related  
commands**

- [ipv6 address](#)
- [ipv6 address autoconfig](#)
- [ipv6 address dhcp](#)
- [ipv6 address \(DHCPv6 PD\)](#)
- [ipv6 dhcp client pd](#)
- [ipv6 nd prefix](#)
- [show ipv6 interface brief](#)
- [show ipv6 route](#)
- [show running-config](#)

# ipv6 eui64-linklocal

**Overview** When IPv6 is enabled on an interface, an EUI link-local address is generated and installed on the interface. In other words, **ipv6 eui64-linklocal** is enabled by default on any IPv6 enabled interface.

Use the **no** variant of this command to disallow the automatic generation of the EUI-64 link-local address on an IPv6 enabled interface.

**Syntax** `ipv6 eui64-linklocal`  
`no ipv6 eui64-linklocal`

**Default** The command **ipv6 eui64-linklocal** is enabled by default on any IPv6 enabled interface.

**Mode** Interface

**Example** To enable IPv6 on an interface eth1, and use the link-local address of fe80::1/10 instead of the EUI-64 link-local that is automatically generated, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# no ipv6 eui64-linklocal
awplus(config-if)# ipv6 address fe80::1/10
```

**Related commands** [ipv6 address](#)  
[ipv6 address autoconfig](#)  
[ipv6 enable](#)

**Command changes** Version 5.4.7-0.1: command added

# ipv6 forwarding

**Overview** Use this command to turn on IPv6 unicast routing for IPv6 packet forwarding. Use this command globally on your device before using the `ipv6 enable` command on individual interfaces. Use the **no** variant of this command to turn off IPv6 unicast routing. Note IPv6 unicast routing is disabled by default.

**Syntax** `ipv6 forwarding`  
`no ipv6 forwarding`

**Mode** Global Configuration

**Default** IPv6 unicast forwarding is disabled by default.

**Usage notes** Enable IPv6 unicast forwarding globally for all interfaces on your device with this command. Use the **no** variant of this command to disable IPv6 unicast forwarding globally for all interfaces on your device.

IPv6 unicast forwarding allows devices to communicate with devices that are more than one hop away, providing that there is a route to the destination address. If IPv6 forwarding is not enabled then pings to addresses on devices that are more than one hop away will fail, even if there is a route to the destination address.

**Examples** To enable IPv6 unicast routing, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
```

To disable IPv6 unicast routing, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 forwarding
```

**Related commands** [ipv6 enable](#)

# ipv6 nd accept-ra-pinfo

**Overview** Use this command to allow the processing of the prefix information included in a received RA (Router Advertisement) on an IPv6 enabled interface.

Use the **no** variant of this command to disable an IPv6 interface from using the prefix information within a received RA.

**Syntax** `ipv6 nd accept-ra-pinfo`  
`no ipv6 nd accept-ra-pinfo`

**Default** The command **ipv6 nd accept-ra-pinfo** is enabled by default on any IPv6 interface.

**Mode** Interface

**Usage notes** By default, when IPv6 is enabled on an interface, SLAAC is also enabled. SLAAC addressing along with the EUI-64 process, uses the prefix information included in a received RA to generate an automatic link-local address on the IPv6 interface.

Note: an AlliedWare Plus device will, by default, add a prefix for the connected interface IPv6 address(es) to the RA it transmits. However, this behavior can be changed by using the command **no ipv6 nd prefix auto-advertise**, so there is no guarantee that an RA will contain a prefix.

**Example** To enable IPv6 on eth1 without installing a SLAAC address on the interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# no ipv6 nd accept-ra-pinfo
```

**Related commands** [ipv6 address](#)  
[ipv6 address autoconfig](#)  
[ipv6 enable](#)

**Command changes** Version 5.4.7-0.1: command added

# ipv6 nd current-hoplimit

**Overview** Use this command to specify the advertised current hop limit used between IPv6 Routers.

Use the **no** variant of this command to reset the current advertised hop limit to its default "0".

**Syntax** `ipv6 nd current-hoplimit <hoplimit>`  
`no ipv6 nd current-hoplimit`

| Parameter                     | Description  |
|-------------------------------|--|
| <code>&lt;hoplimit&gt;</code> | Specifies the advertised current hop limit value. Valid values are from 0 to 255 hops. |

**Default** 0 (No advertised current hop limit specified)

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Examples** To set the advertised current hop limit to 2 between IPv6 Routers on vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 nd current-hoplimit 2
```

To reset the advertised current hop limit to the default 0 on vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 nd current-hoplimit
```

To set the advertised current hop limit to 2 between IPv6 Routers on ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd current-hoplimit 2
```

To reset the advertised current hop limit to the default 0 on ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 nd current-hoplimit
```

**Related commands** [ipv6 nd managed-config-flag](#)  
[ipv6 nd prefix](#)  
[ipv6 nd suppress-ra](#)

# ipv6 nd managed-config-flag

**Overview** Use this command to set the managed address configuration flag, contained within the router advertisement field.

Setting this flag indicates the operation of a stateful autoconfiguration protocol such as DHCPv6 for address autoconfiguration, and that address information (i.e. the network prefix) and other (non-address) information can be requested from the device.

An unset flag enables hosts receiving the advertisements to use a stateless autoconfiguration mechanism to establish their IPv6 addresses. The default is flag unset.

Use the **no** variant of this command to reset this command to its default of having the flag unset.

**Syntax** `ipv6 nd managed-config-flag`  
`no ipv6 nd managed-config-flag`

**Default** Unset

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** Advertisement flags will not be transmitted unless you have applied the [ipv6 nd suppress-ra](#) command. This step is included in the example below.

**Example** To set the managed address configuration flag on the VLAN interface `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 nd managed-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

To set the managed address configuration flag on the PPP interface `ppp0`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd managed-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

**Related commands** [ipv6 nd suppress-ra](#)  
[ipv6 nd prefix](#)  
[ipv6 nd other-config-flag](#)



# ipv6 nd minimum-ra-interval

**Overview** Use this command in Interface Configuration mode to set a minimum Router Advertisement (RA) interval for 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`

| Parameter                    | Description  |
|------------------------------|--|
| <code>&lt;seconds&gt;</code> | Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 3 to 1350 seconds. |

**Default** The RA interval for a VLAN interface is unset by default.

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Examples** To set the minimum RA interval for the VLAN interface `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 nd minimum-ra-interval 60
```

To remove the minimum RA interval for the VLAN interface `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 nd minimum-ra-interval
```

To set the minimum RA interval for the PPP interface `ppp0`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd minimum-ra-interval 60
```

To remove the minimum RA interval for the PPP interface `ppp0`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 nd minimum-ra-interval
```

**Related commands**

- ipv6 nd ra-interval
- ipv6 nd suppress-ra
- ipv6 nd prefix
- ipv6 nd other-config-flag

# ipv6 nd other-config-flag

**Overview** Use this command to set the **other** stateful configuration flag (contained within the router advertisement field) to be used for IPv6 address auto-configuration. This flag is used to request the router to provide information in addition to providing addresses.

Setting the `ipv6 nd managed-config-flag` command implies that the `ipv6 nd other-config-flag` will also be set.

Use **no** variant of this command to reset the value to the default.

**Syntax** `ipv6 nd other-config-flag`  
`no ipv6 nd other-config-flag`

**Default** Unset

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** Advertisement flags will not be transmitted unless you have applied the `ipv6 nd suppress-ra` command. This step is included in the example below.

**Example** To set the IPv6 other-config-flag on the VLAN interface vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 nd other-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

To set the IPv6 other-config-flag on the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd other-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

**Related commands** `ipv6 nd suppress-ra`  
`ipv6 nd prefix`  
`ipv6 nd managed-config-flag`

# ipv6 nd prefix

**Overview** Use this command in Interface Configuration mode 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**

```

ipv6 nd prefix <ipv6-prefix/length>
ipv6 nd prefix <ipv6-prefix/length> [<valid-lifetime>]
ipv6 nd prefix <ipv6-prefix/length>
<valid-lifetime><preferred-lifetime> [no-autoconfig]
ipv6 nd prefix <ipv6-prefix/length>
<valid-lifetime><preferred-lifetime> off-link [no-autoconfig]
no ipv6 nd prefix [<ipv6-addr/prefix-length>|all]

```

| Parameter                         | Description   |
|-----------------------------------|---|
| <i>&lt;ipv6-prefix/length&gt;</i> | The prefix to be advertised by the router advertisement message.<br>The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64. The default is X:X::/64.  |
| <i>&lt;valid-lifetime&gt;</i>     | The the period during which the specified IPv6 address prefix is valid. This can be set to a value between 0 and 4294967295 seconds. The default is 2592000 (30 days). Note that this period should be set to a value greater than that set for the prefix preferred-lifetime.  |
| <i>&lt;preferred-lifetime&gt;</i> | Specifies the IPv6 prefix preferred lifetime. This is the period during which the IPv6 address prefix is considered a current (undeprecated) value. After this period, the command is still valid but should not be used in new communications. Set to a value between 0 and 4294967295 seconds. The default is 604800 seconds (7 days). Note that this period should be set to a value less than that set for the prefix valid-lifetime. |
| off-link                          | Specify the IPv6 prefix off-link flag. The default is flag set.   |
| no-autoconfig                     | Specify the IPv6 prefix no autoconfiguration flag. Setting this flag indicates that the prefix is not to be used for autoconfiguration. The default is flag set.  |
| all                               | Specify all IPv6 prefixes associated with the VLAN interface.   |

**Default** Valid-lifetime default is 2592000 seconds (30 days). Preferred-lifetime default is 604800 seconds (7 days).

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** This command specifies the IPv6 prefix flags that are advertised by the router advertisement message.

**Examples** To configure the device to issue router advertisements on vlan1, and advertise the address prefix of 2001:0db8::/64, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64
```

To configure the router to issue router advertisements on ppp0, and advertise the address prefix of 2001:0db8::/64, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64
```

To configure the device to issue router advertisements on vlan1, and advertise the address prefix of 2001:0db8::/64 with a valid lifetime of 10 days and a preferred lifetime of 5 days, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
```

To configure the device to issue router advertisements on vlan1 and advertise the address prefix of 2001:0db8::/64 with a valid lifetime of 10 days, a preferred lifetime of 5 days, and no prefix used for autoconfiguration, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
no-autoconfig
```

To reset router advertisements on vlan1, so the address prefix of 2001:0db8::/64 is not advertised from the device, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/64
```

To reset all router advertisements on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 nd prefix all
```

**Related commands** [ipv6 nd suppress-ra](#)

# ipv6 nd proxy interface

**Overview** Use this command to enable the neighbor discovery proxy that forwards Neighbor Solicitations (NS) and Neighbor Advertisements (NA) between two interfaces.

Use the **no** variant of this command to disable the neighbor discovery proxy.

**Syntax** `ipv6 nd proxy interface [<interface-name>]`  
`no ipv6 nd proxy`

| Parameter        | Description   |
|------------------|---|
| <interface-name> | The name of the VLAN, Ethernet or Bridge interface to proxy NS and NA from/to. For example <i>vlan1</i> , <i>eth1</i> or <i>br1</i> . |

**Default** No ND proxy is enabled

**Mode** Interface Configuration

**Examples** To enable neighbor discovery proxy on eth1 and forward NS and NA to vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd proxy interface vlan1
```

To disable neighbor discovery proxy on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 nd proxy
```

**Related commands** [show running-config](#)

**Command changes** Version 5.4.8-1.1: command added

# ipv6 nd ra-interval

**Overview** Use this command to specify the interval between IPv6 Router Advertisements (RA) transmissions.

Use **no** parameter with this command to reset the value to the default value (600 seconds).

**Syntax** `ipv6 nd ra-interval <seconds>`  
`no ipv6 nd ra-interval`

| Parameter                    | Description  |
|------------------------------|--|
| <code>&lt;seconds&gt;</code> | Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 4 to 1800 seconds. |

**Default** 600 seconds.

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** 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 `vlan1` to be 60 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 nd ra-interval 60
awplus(config-if)# no ipv6 nd suppress-ra
```

**Related commands** [ipv6 nd minimum-ra-interval](#)  
[ipv6 nd suppress-ra](#)  
[ipv6 nd prefix](#)

# ipv6 nd ra-lifetime

**Overview** Use this command to specify the time period that this router can usefully act as a default gateway for the network. Each router advertisement resets this time period.

Use **no** parameter with this command to reset the value to default.

**Syntax** `ipv6 nd ra-lifetime <seconds>`  
`no ipv6 nd ra-lifetime`

| Parameter                    | Description  |
|------------------------------|--|
| <code>&lt;seconds&gt;</code> | 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 <a href="#">ipv6 nd ra-interval</a> command. |

**Default** 1800 seconds

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** This command specifies the lifetime of the current router to be announced in IPv6 Router Advertisements.

Advertisement flags will not be transmitted unless you have applied the [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 `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 nd ra-lifetime 8000
awplus(config-if)# no ipv6 nd suppress-ra
```

To set the advertisement lifetime of 8000 seconds on the PPP interface `ppp0`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd ra-lifetime 8000
awplus(config-if)# no ipv6 nd suppress-ra
```

**Related commands** [ipv6 nd suppress-ra](#)  
[ipv6 nd prefix](#)



# ipv6 nd reachable-time

**Overview** Use this command to specify the reachable time in the router advertisement to be used for detecting reachability of the IPv6 neighbor.

Use the **no** variant of this command to reset the value to default.

**Syntax** `ipv6 nd reachable-time <milliseconds>`  
`no ipv6 nd reachable-time`

| Parameter      | Description   |
|----------------|---|
| <milliseconds> | Time period in milliseconds. Valid values are from 1000 to 3600000.<br>Setting this value to 0 indicates an unspecified reachable-time. |

**Default** 0 milliseconds

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** This command specifies the reachable time of the current router to be announced in IPv6 Router Advertisements.

Advertisement flags will not be transmitted unless you have applied the `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 vlan1 to be 1800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
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 vlan1 to an unspecified reachable-time (0 milliseconds), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 nd reachable-time
```

To set the reachable-time in router advertisements on the PPP interface ppp0 to be 1800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd reachable-time 1800000
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the reachable-time in router advertisements on the PPP interface ppp0 to an unspecified reachable-time (0 milliseconds), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 nd reachable-time
```

**Related commands**

- [ipv6 nd suppress-ra](#)
- [ipv6 nd prefix](#)

# ipv6 nd retransmission-time

**Overview** Use this command to specify the advertised retransmission interval for Neighbor Solicitation in milliseconds between IPv6 Routers.

Use the **no** variant of this command to reset the retransmission time to the default (1 second).

**Syntax** `ipv6 nd retransmission-time <milliseconds>`  
`no ipv6 nd retransmission-time`

| Parameter                         | Description   |
|-----------------------------------|---|
| <code>&lt;milliseconds&gt;</code> | Time period in milliseconds. Valid values are from 1000 to 3600000. |

**Default** 1000 milliseconds (1 second)

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Examples** To set the retransmission-time of Neighbor Solicitation on the VLAN interface `vlan1` to be 800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 nd retransmission-time 800000
```

To reset the retransmission-time of Neighbor Solicitation on the VLAN interface `vlan1` to the default 1000 milliseconds (1 second), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 nd retransmission-time
```

To set the retransmission-time of Neighbor Solicitation on the PPP interface `ppp0` to be 800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd retransmission-time 800000
```

To reset the retransmission-time of Neighbor Solicitation on the PPP interface `ppp0` to the default 1000 milliseconds (1 second), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 nd retransmission-time
```

**Related  
commands** [ipv6 nd suppress-ra](#)  
[ipv6 nd prefix](#)

# ipv6 nd 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 or a PPP interface.

**Example** To enable the transmission of router advertisements from vlan1 on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 nd suppress-ra
```

To enable the transmission of router advertisements from ppp0 on the router, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 nd suppress-ra
```

**Related commands** [ipv6 nd ra-interval](#)  
[ipv6 nd prefix](#)

# ipv6 neighbor

**Overview** Use this command to add a static IPv6 neighbor entry.  
Use the **no** variant of this command to remove a specific IPv6 neighbor entry.

**Syntax** `ipv6 neighbor <ipv6-address> <vlan-name> <mac-address>  
<port-list>`  
`no ipv6 neighbor <ipv6-address> <vlan-name> <port-list>`

| Parameter                         | Description  |
|-----------------------------------|--|
| <code>&lt;ipv6-address&gt;</code> | Specify the neighbor's IPv6 address in the format X:X::X:X.                            |
| <code>&lt;vlan-name&gt;</code>    | Specify the neighbor's VLAN name.  |
| <code>&lt;mac-address&gt;</code>  | Specify the MAC hardware address in hexadecimal notation in the format HHHH.HHHH.HHHH. |
| <code>&lt;port-list&gt;</code>    | Specify the port number, or port range.  |

**Mode** Global Configuration

**Usage notes** Use this command to clear a specific IPv6 neighbor entry. To clear all dynamic address entries, use the [clear ipv6 neighbors](#) command.

**Example** To create a static neighbor entry for IPv6 address 2001:0db8::a2, on vlan1, with MAC address 0000.cd28.0880, on port1.0.1, use the command:

```
awplus# configure terminal
awplus(config)# ipv6 neighbor 2001:0db8::a2 vlan1
0000.cd28.0880 port1.0.1
```

**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 notes** When opportunistic neighbor discovery is enabled, the device will reply to any received unsolicited ICMPv6 ND packets. The source MAC address for the unsolicited ICMPv6 ND packet is added to the IPv6 ND cache, so the device forwards the ICMPv6 ND packet. When opportunistic neighbor discovery is disabled, the source MAC address for the ICMPv6 packet is not added to the IPv6 ND cache, so the ICMPv6 ND packet is not forwarded by the device.

**Examples** To enable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# ipv6 opportunistic-nd
```

To disable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# no ipv6 opportunistic-nd
```

**Related commands** [arp opportunistic-nd](#)  
[show ipv6 neighbors](#)  
[show running-config interface](#)

# ipv6 route

**Overview** This command adds a static IPv6 route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to advertise routes to neighbors and forward packets.

The **no** variant of this command removes the static route.

**Syntax** `ipv6 route <dest-prefix> <dest-prefix/length> {<gateway-ip>|<gateway-name>} [<distvalue>]`  
`no ipv6 route <dest-prefix> <dest-prefix/length> {<gateway-ip>|<gateway-name>} [<distvalue>]`

| Parameter                               | Description   |
|---|---|
| <code>&lt;dest-prefix/length&gt;</code> | Specifies the IP destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.        |
| <code>&lt;gateway-ip&gt;</code>         | Specifies the IP gateway (or next hop) address. The IPv6 address uses the format X:X::X/X/Prefix-Length. The prefix-length is usually set between 0 and 64. |
| <code>&lt;gateway-name&gt;</code>       | Specifies the name of the gateway (or next hop) interface.  |
| <code>&lt;distvalue&gt;</code>          | Specifies the administrative distance for the route. Valid values are from 1 to 255.  |

**Mode** Global Configuration

**Usage notes** You can use administrative distance to determine which routes take priority over other routes.

**Example** `awplus# configure terminal`  
`awplus(config)# ipv6 route 2001:0db8::1/128 vlan1 32`

**Validation Commands** `show running-config`  
`show ipv6 route`



# ipv6 unreachable

**Overview** Use this command to enable ICMPv6 (Internet Control Message Protocol version 6) type 1, destination unreachable, messages.

Use the **no** variant of this command to disable destination unreachable messages. This prevents an attacker from using these messages to discover the topology of a network.

**Syntax** `ipv6 unreachable`  
`no ipv6 unreachable`

**Default** Destination unreachable messages are enabled by default.

**Mode** Global Configuration

**Usage notes** When a device receives a packet for a destination that is unreachable it returns an ICMPv6 type 1 message. This message includes a reason code, as per the table below. An attacker can use these messages to obtain information regarding the topology of a network. Disabling destination unreachable messages, using the **no ipv6 unreachable** command, secures your network against this type of probing.

**NOTE:** *Disabling ICMPv6 destination unreachable messages breaks applications such as traceroute, which depend on these messages to operate correctly.*

Table 16-1: ICMPv6 type 1 reason codes and description

| Code | Description [RFC]  |
|------|--|
| 0    | No route to destination [RFC4443]                                    |
| 1    | Communication with destination administratively prohibited [RFC4443] |
| 2    | Beyond scope of source address [RFC4443]                             |
| 3    | Address unreachable [RFC4443]  |
| 4    | Port unreachable [RFC4443]   |
| 5    | Source address failed ingress/egress policy [RFC4443]                |
| 6    | Reject route to destination [RFC4443]                                |
| 7    | Error in Source Routing Header [RFC6554]                             |

**Example** To disable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# no ipv6 unreachable
```

To enable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# ipv6 unreachable
```

# optimistic-nd

**Overview** Use this command to enable the optimistic neighbor discovery feature for both IPv4 and IPv6.

Use the **no** variant of this command to disable the optimistic neighbor discovery feature.

**Syntax** `optimistic-nd`  
`no optimistic-nd`

**Default** The optimistic neighbor discovery feature is enabled by default.

**Mode** Interface Configuration for a VLAN interface.

**Usage notes** The optimistic neighbor discovery feature allows the device, after learning an IPv4 or IPv6 neighbor, to refresh the neighbour before it is deleted from the ARP or neighbour tables. The optimistic neighbor discovery feature enables the device to sustain L3 traffic switching to a neighbor without interruption.

If a neighbor receiving optimistic neighbor solicitations does not answer optimistic neighbor solicitations with neighbor advertisements, then the device puts the neighbour entry into the "stale" state, and subsequently deletes it from the L3 switching tables.

**Examples** To enable the optimistic neighbor discovery feature on vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# optimistic-nd
```

To disable the optimistic neighbor discovery feature on vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no optimistic-nd
```

**Related commands** [show running-config](#)

# ping ipv6

**Overview** This command sends a query to another IPv6 host (send Echo Request messages).

**Syntax** `ping ipv6 {<host>|<ipv6-address>} [repeat {<1-2147483647>|continuous}] [size <10-1452>] [interface <interface-list>] [timeout <1-65535>]`

| Parameter                                     | Description   |
|---|---|
| <code>&lt;ipv6-addr&gt;</code>                | The destination IPv6 address. The IPv6 address uses the format X:X::X:X.  |
| <code>&lt;hostname&gt;</code>                 | The destination hostname.   |
| <code>repeat</code>                           | Specify the number of ping packets to send.   |
| <code>&lt;1-2147483647&gt;</code>             | Specify repeat count. The default is 5.   |
| <code>size &lt;10-1452&gt;</code>             | The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).   |
| <code>interface &lt;interface-list&gt;</code> | <p>The interface or range of configured IP interfaces to use as the source in the IP header of the ping packet. The interface can be one of:</p> <ul style="list-style-type: none"> <li>• a PPP interface (e.g. ppp0)</li> <li>• an Eth interface (e.g. eth1)</li> <li>• vlan1</li> <li>• a bridge interface (e.g. br0)</li> <li>• a tunnel interface (e.g. tunnel0)</li> <li>• a WWAN interface (e.g. wwan0)</li> <li>• the loopback interface (lo)</li> <li>• a continuous range of interfaces, separated by a hyphen (e.g. ppp2-4)</li> <li>• a comma-separated list (e.g. ppp0,ppp2-4). Do not mix interface types in a list.</li> </ul> <p>You can only specify the interface when pinging a link local address.</p> |
| <code>timeout &lt;1-65535&gt;</code>          | 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.  |
| <code>repeat</code>                           | Specify the number of ping packets to send.   |
| <code>&lt;1-2147483647&gt;</code>             | Specify repeat count. The default is 5.   |
| <code>continuous</code>                       | Continuous ping.  |

| Parameter            | Description  |
|----------------------|--|
| size <10-1452>       | The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).  |
| timeout<br><1-65535> | The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait. |

**Mode** User Exec and Privileged Exec

**Example** awplus# ping ipv6 2001:0db8::a2

**Related commands** [traceroute ipv6](#)

# show ipv6 forwarding

**Overview** Use this command to display IPv6 forwarding status.

**Syntax** `show ipv6 forwarding`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ipv6 forwarding`

**Output** Figure 16-1: 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 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 16-2: Example output from the **show ipv6 interface brief** command

```
awplus#show ipv6 interface brief
Interface      IPv6-Address          Status      Protocol
lo             unassigned           admin up   running
vlan1         2001:db8::1/48      admin up   down
              fe80::215:77ff:fee9:5c50/64
```

**Related commands** [show interface brief](#)

# show ipv6 neighbors

**Overview** Use this command to display all IPv6 neighbors.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show ipv6 neighbors`

**Mode** User Exec and Privileged Exec

# show ipv6 route

**Overview** Use this command to display the IPv6 routing table for a protocol or from a particular table.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 route`  
`[connected|database|static|summary|<ipv6-address>|`  
`<ipv6-addr/prefix-length>]`

| Parameter            | Description  |
|----------------------|--|
| connected            | Displays only the routes learned from connected interfaces.  |
| database             | Displays only the IPv6 routing information extracted from the database.  |
| static               | Displays only the IPv6 static routes you have configured.  |
| summary              | Displays summary information from the IPv6 routing table.  |
| <ipv6-address>       | Displays the routes for the specified address in the IP routing table. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64. |
| <ipv6-prefix/length> | Displays only the routes for the specified IP prefix.  |

**Mode** User Exec and Privileged Exec

**Example** To display an IP route with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

To display all database entries for an IP route, use the following command:

```
awplus# show ipv6 route database
```

**Output** Figure 16-3: Example output of the **show ipv6 route database** command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
> - selected route, * - FIB route, p - stale info
Timers: Uptime

S   ::/0 [1/0] via 2001::a:0:0:c0a8:a01 inactive, 6d22h12m
      [1/0] via 2001::fa:0:0:c0a8:fa01 inactive, 6d22h12m
```



# show ipv6 route summary

**Overview** Use this command to display the summary of the current NSM RIB entries.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 route summary`

**Mode** User Exec and Privileged Exec

**Example** To display IP route summary, use the following command:

```
awplus# show ipv6 route summary
```

**Output** Figure 16-4: Example output from the **show ipv6 route summary** command

```
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths is 4
RouteSource      Networks
connected        4
Total            4
FIB              0
```

**Related commands** [show ip route database](#)

# traceroute ipv6

**Overview** Use this command to trace the route to the specified IPv6 host.

**Syntax** `traceroute ipv6 {<ipv6-addr>|<hostname>}`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;ipv6-addr&gt;</code> | The destination IPv6 address. The IPv6 address uses the format X:X::X:X. |
| <code>&lt;hostname&gt;</code>  | The destination hostname.  |

**Mode** User Exec and Privileged Exec

**Example** To run a traceroute for the IPv6 address 2001:0db8::a2, use the following command:

```
awplus# traceroute ipv6 2001:0db8::a2
```

**Related commands** [ping ipv6](#)

# 17

# Routing Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of routing commands that are common across the routing IP protocols. For more information, see the [Route Selection Feature Overview and Configuration Guide](#).

- Command List**
- [“ip route”](#) on page 612
  - [“ipv6 route”](#) on page 614
  - [“max-fib-routes”](#) on page 615
  - [“max-static-routes”](#) on page 616
  - [“maximum-paths”](#) on page 617
  - [“show ip route”](#) on page 618
  - [“show ip route database”](#) on page 620
  - [“show ip route summary”](#) on page 621
  - [“show ipv6 route”](#) on page 622
  - [“show ipv6 route summary”](#) on page 623

# ip route

**Overview** This command adds a static route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to advertise routes to neighbors and forward packets.

The **no** variant of this command removes the static route from the RIB and FIB.

**Syntax** `ip route <subnet&mask> {<gateway-ip>|<interface>} [<distance>]`  
`no ip route <subnet&mask> {<gateway-ip>|<interface>} [<distance>]`

| Parameter     | Description   |
|---------------|---|
| <subnet&mask> | The IPv4 address of the destination subnet defined using either a prefix length or a separate mask specified in one of the following formats: <ul style="list-style-type: none"> <li>The IPv4 subnet address in dotted decimal notation followed by the subnet mask, also in dotted decimal notation.</li> <li>The IPv4 subnet address in dotted decimal notation, followed by a forward slash, then the prefix length</li> </ul> |
| <gateway-ip>  | The IPv4 address of the gateway device.   |
| <interface>   | The interface that connects your device to the network. Enter the name of the VLAN or its VID. You can also enter 'null' as an interface. Specify a 'null' interface to add a null or blackhole route to the device.<br>The gateway IP address or the interface is required.  |
| <distance>    | The administrative distance for the static route in the range <1-255>. Static routes by default have an administrative distance of 1, which gives them the highest priority possible.   |

**Mode** Global Configuration

**Default** The default administrative distance for a static route is 1.

**Usage notes** You can use administrative distance to determine which routes take priority over other routes.

Specify a 'Null' interface to add a null or blackhole route to the switch. A null or blackhole route is a routing table entry that does not forward packets, so any packets sent to it are dropped.

**Examples** To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at "10.10.0.2" with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To remove the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at "10.10.0.2" with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# no ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To specify a null or blackhole route 192.168.4.0/24, so packets forwarded to this route are dropped, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.4.0/24 null
```

To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at "10.10.0.2" with an administrative distance of 128, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
128
```

**Related commands** [show ip route](#)  
[show ip route database](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# ipv6 route

**Overview** This command adds a static IPv6 route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to advertise routes to neighbors and forward packets.

The **no** variant of this command removes the static route.

**Syntax** `ipv6 route <dest-prefix> <dest-prefix/length> {<gateway-ip>|<gateway-name>} [<distvalue>]`  
`no ipv6 route <dest-prefix> <dest-prefix/length> {<gateway-ip>|<gateway-name>} [<distvalue>]`

| Parameter                               | Description   |
|---|---|
| <code>&lt;dest-prefix/length&gt;</code> | Specifies the IP destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.      |
| <code>&lt;gateway-ip&gt;</code>         | Specifies the IP gateway (or next hop) address. The IPv6 address uses the format X:X::X:Prefix-Length. The prefix-length is usually set between 0 and 64. |
| <code>&lt;gateway-name&gt;</code>       | Specifies the name of the gateway (or next hop) interface.  |
| <code>&lt;distvalue&gt;</code>          | Specifies the administrative distance for the route. Valid values are from 1 to 255.  |

**Mode** Global Configuration

**Usage notes** You can use administrative distance to determine which routes take priority over other routes.

**Example**

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 vlan1 32
```

**Validation Commands** `show running-config`  
`show ipv6 route`

# max-fib-routes

**Overview** This command enables you to control the maximum number of FIB routes configured. It operates by providing parameters that enable you to configure preset maximums and warning message thresholds.

**NOTE:** For static routes use the *max-static-routes* command.

Use the **no** variant of this command to set the maximum number of FIB routes to the default of 4294967294 FIB routes.

**Syntax** `max-fib-routes <1-4294967294> [<1-100>|warning-only]`  
`no max-fib-routes`

| Parameter                         | Description  |
|-----------------------------------|--|
| <code>max-fib-routes</code>       | This is the maximum number of routes that can be stored in the device's Forwarding Information dataBase. In practice, other practical system limits would prevent this maximum being reached.  |
| <code>&lt;1-4294967294&gt;</code> | The allowable configurable range for setting the maximum number of FIB-routes.   |
| <code>&lt;1-100&gt;</code>        | This parameter enables you to optionally apply a percentage value. This percentage will be based on the maximum number of FIB routes you have specified. This will cause a warning message to appear when your routes reach your specified percentage value. Routes can continue to be added until your configured maximum value is reached. |
| <code>warning-only</code>         | This parameter enables you to optionally apply a warning message. If you set this option a warning message will appear if your maximum configured value is reached. Routes can continue to be added until your device reaches either the maximum capacity value of 4294967294, or a practical system limit.                                  |

**Default** The default number of FIB routes is the maximum number of FIB routes (4294967294).

**Mode** Global Configuration

**Examples** To set the maximum number of dynamic routes to 2000 and warning threshold of 75%, use the following commands:

```
awplus# config terminal
awplus(config)# max-fib-routes 2000 75
```

# max-static-routes

**Overview** Use this command to set the maximum number of static routes, excluding FIB (Forwarding Information Base) routes.

**NOTE:** For FIB routes use the [max-fib-routes](#) command.

Use the **no** variant of this command to set the maximum number of static routes to the default of 1024 static routes.

**Syntax** `max-static-routes <1-1024>`  
`no max-static-routes`

**Default** The default number of static routes is the maximum number of static routes (1024).

**Mode** Global Configuration

**Example** To reset the maximum number of static routes to the default maximum, use the command:

```
awplus# configure terminal
awplus(config)# no max-static-routes
```

**NOTE:** Static routes are applied before adding routes to the RIB (Routing Information Base). Therefore, rejected static routes will not appear in the running config.

**Related commands** [max-fib-routes](#)



# maximum-paths

**Overview** This command enables ECMP on your device, and sets the maximum number of paths that each route has in the Forwarding Information Base (FIB). ECMP is enabled by default.

The **no** variant of this command sets the maximum paths to the default of 4.

ECMP path calculations are flow-based. This means that packets from the same flow will always be sent on the same path.

**Syntax** `maximum-paths <1-8>`  
`no maximum-paths`

| Parameter | Description   |
|-----------|---|
| <1-8>     | The maximum number of paths that a route can have in the FIB. |

**Default** By default the maximum number of paths is 4.

**Mode** Global Configuration

**Examples** To set the maximum number of paths for each route in the FIB to 5, use the 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|static|<ip-addr>|<ip-addr/prefix-length>]`

| Parameter                                  | Description   |
|--|---|
| <code>connected</code>                     | Displays only the routes learned from connected interfaces.                             |
| <code>static</code>                        | Displays only the static routes you have configured.                                    |
| <code>&lt;ip-addr&gt;</code>               | Displays the routes for the specified address. Enter an IPv4 address.                   |
| <code>&lt;ip-addr/prefix-length&gt;</code> | Displays the routes for the specified network. Enter an IPv4 address and prefix length. |

**Mode** User Exec and Privileged Exec

**Example** To display the static routes in the FIB, use the command:

```
awplus# show ip route static
```

**Output** Each entry in the output from this command has a code preceding it, indicating the source of the routing entry. The first few lines of the output list the possible codes that may be seen with the route entries.

Typically, route entries are composed of the following elements:

- code
- a second label indicating the sub-type of the route
- network or host IP address
- administrative distance and metric
- next hop IP address
- outgoing interface name
- time since route entry was added

Figure 17-1: Example output from the **show ip route** command

```
awplus#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, D - DHCP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default

S      10.32.18.135/32 [1/0] via 10.37.163.129, vlan1
S      10.33.0.0/16 [1/0] via 10.37.163.129, vlan1
C      10.37.163.128/27 is directly connected, vlan1
S      11.1.1.0/24 [1/0] via 12.1.1.1, eth1
C      12.1.1.0/24 is directly connected, eth1
C      192.169.1.0/30 is directly connected, tunnel1
C      192.169.40.0/30 is directly connected, tunnel4444

Gateway of last resort is not set
```

**Connected Route** The connected route entry consists of:

```
C      10.10.31.0/24 is directly connected, eth1
```

This route entry denotes:

- Route entries for network 10.10.31.0/24 are derived from the IP address of local interface eth1.
- These routes are marked as Connected routes (C) and always preferred over routes for the same network learned from other routing protocols.

**Related commands** [ip route](#)  
[maximum-paths](#)  
[show ip route database](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# show ip route database

**Overview** This command displays the routing entries in the RIB (Routing Information Base).

When multiple entries are available for the same prefix, RIB uses the routes' administrative distances to choose the best route. All best routes are entered into the FIB (Forwarding Information Base). To view the routes in the FIB, use the [show ip route](#) command.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > output redirection token.

**Syntax** `show ip route database [connected|static]`

| Parameter | Description   |
|-----------|---|
| connected | Displays only the routes learned from connected interfaces. |
| static    | Displays only the static routes you have configured.        |

**Mode** User Exec and Privileged Exec

**Example** To display the static routes in the RIB, use the command:

```
awplus# show ip route database static
```

**Output** Figure 17-2: Example output from the **show ip route database** command

```
awplus#show ip route database
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, D - DHCP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       > - selected route, * - FIB route, p - stale info

S    *> 0.0.0.0/0 [1/0] via 10.34.1.1, vlan1
C    *> 10.34.0.0/16 is directly connected, vlan1
S    192.168.2.0/24 [1/0] is directly connected, eth1 inactive

Gateway of last resort is not set
```

**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 17-3: Example output from the **show ip route summary** command

```
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source      Networks
connected         5
Total             8
```

**Related commands** [show ip route](#)  
[show ip route database](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# show ipv6 route

**Overview** Use this command to display the IPv6 routing table for a protocol or from a particular table.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 route`  
`[connected|database|static|summary|<ipv6-address>|`  
`<ipv6-addr/prefix-length>]`

| Parameter            | Description  |
|----------------------|--|
| connected            | Displays only the routes learned from connected interfaces.  |
| database             | Displays only the IPv6 routing information extracted from the database.  |
| static               | Displays only the IPv6 static routes you have configured.  |
| summary              | Displays summary information from the IPv6 routing table.  |
| <ipv6-address>       | Displays the routes for the specified address in the IP routing table. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64. |
| <ipv6-prefix/length> | Displays only the routes for the specified IP prefix.  |

**Mode** User Exec and Privileged Exec

**Example** To display an IP route with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

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, B - BGP
> - selected route, * - FIB route, p - stale info
Timers: Uptime

S   ::/0 [1/0] via 2001::a:0:0:c0a8:a01 inactive, 6d22h12m
      [1/0] via 2001::fa:0:0:c0a8:fa01 inactive, 6d22h12m
```

# show ipv6 route summary

**Overview** Use this command to display the summary of the current NSM RIB entries.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 route summary`

**Mode** User Exec and Privileged Exec

**Example** To display IP route summary, use the following command:

```
awplus# show ipv6 route summary
```

**Output** Figure 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
Total            4
FIB              0
```

**Related commands** [show ip route database](#)

# Part 4: Access and Security



# 18

# Public Key Infrastructure Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure the Public Key Infrastructure (PKI) capabilities on an AlliedWare Plus device. For more information about PKI, see the [Public Key Infrastructure \(PKI\) Feature Overview and Configuration Guide](#).

- Command List**
- [“crypto key generate rsa”](#) on page 626
  - [“crypto key zeroize”](#) on page 627
  - [“crypto pki authenticate”](#) on page 628
  - [“crypto pki enroll”](#) on page 629
  - [“crypto pki export pem”](#) on page 630
  - [“crypto pki export pkcs12”](#) on page 631
  - [“crypto pki import pem”](#) on page 632
  - [“crypto pki import pkcs12”](#) on page 634
  - [“crypto pki trustpoint”](#) on page 635
  - [“enrollment \(ca-trustpoint\)”](#) on page 636
  - [“fingerprint \(ca-trustpoint\)”](#) on page 637
  - [“no crypto pki certificate”](#) on page 639
  - [“rsakeypair \(ca-trustpoint\)”](#) on page 640
  - [“show crypto key mypubkey rsa”](#) on page 641
  - [“show crypto pki certificates”](#) on page 642
  - [“show crypto pki trustpoint”](#) on page 644
  - [“subject-name \(ca-trustpoint\)”](#) on page 645

# crypto key generate rsa

**Overview** Use this command to generate a cryptographic public/private key pair for the Rivest-Shamir-Adleman (RSA) encryption algorithm.

**Syntax** `crypto key generate rsa [label <keylabel>] [<1024-4096>]`

| Parameter   | Description   |
|-------------|---|
| <keylabel>  | The name of the key to be created. The name must start with an alphanumeric character, and may only contain alphanumeric characters, underscores, dashes, or periods. The maximum length of the name is 63 characters. If no label is specified the default value "server-default" is used. |
| <1024-4096> | The bit length for the key. If no bit length is specified the default of 2048 is used.  |

**Mode** Privileged Exec

**Usage notes** The generated key may be used for multiple server certificates in the system. A key is referenced by its label. A bit length between 1024 and 4096 bits may be specified. Larger bit lengths are more secure, but require more computation time. The specified key must not already exist.

**Example** To create a key with the label "example-server-key" and a bit length of 2048, use the commands:

```
awplus> enable  
awplus# crypto key generate rsa label example-server-key 2048
```

**Related commands** [crypto key zeroize](#)  
[rsakeypair \(ca-trustpoint\)](#)  
[show crypto key mypubkey rsa](#)

# crypto key zeroize

**Overview** Use this command to delete one or all cryptographic public/private key pairs.

**Syntax** `crypto key zeroize rsa <keylabel>`  
`crypto key zeroize all`

| Parameter                         | Description  |
|-----------------------------------|--|
| <code>rsa &lt;keylabel&gt;</code> | Delete a single key pair for the Rivest-Shamir-Adleman (RSA) encryption algorithm. |
| <code>all</code>                  | Delete all keys.   |

**Mode** Privileged Exec

**Usage notes** Note that this command has the same effect as using the **delete** command (it deletes the file from Flash memory but does not overwrite it with zeros).

The specified key must exist but must not be in use for any existing server certificates.

A key may not be deleted if it is associated with the server certificate or server certificate signing request for an existing trustpoint. To remove a server certificate so that the key may be deleted, use the **no crypto pki enroll** command to de-enroll the server.

**Example** To delete an RSA key named "example-server-key", use the following command:

```
awplus# crypto key zeroize rsa example-server-key
```

**Related commands** [crypto key generate rsa](#)  
[show crypto key mypubkey rsa](#)

**Command changes** Version 5.4.6-1.1: zeroize functionality added to x930 Series  
Version 5.4.8-1.2: zeroize functionality added to x220, XS900MX, x550 Series  
Version 5.4.8-2.1: zeroize functionality added to SBx908 GEN2, x950 Series

# crypto pki authenticate

**Overview** Use this command to authenticate a trustpoint by generating or importing the root CA certificate. This must be done before the server can be enrolled to the trustpoint.

**Syntax** `crypto pki authenticate <trustpoint>`

| Parameter                       | Description                                     |
|---------------------------------|---|
| <code>&lt;trustpoint&gt;</code> | The name of the trustpoint to be authenticated. |

**Mode** Privileged Exec

**Usage notes** If the trustpoint's **enrollment** setting is "selfsigned", then this command causes a private key to be generated for the root CA, and a self-signed certificate to be generated based on that key.

If the trustpoint's **enrollment** setting is "terminal", then this command prompts the user to paste a certificate Privacy Enhanced Mail (PEM) file at the CLI terminal. If the certificate is a valid selfsigned CA certificate, then it will be stored as the trustpoint's root CA certificate.

The specified trustpoint must already exist, and its enrollment mode must have been defined.

**Example** To show the **enrollment** setting of a trustpoint named "example" and then generate a certificate from it, use the commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# enrollment selfsigned
awplus(config)# exit
awplus# exit
awplus# crypto pki authenticate example
```

**Related commands**

- [crypto pki import pem](#)
- [crypto pki trustpoint](#)
- [enrollment \(ca-trustpoint\)](#)

# crypto pki enroll

**Overview** Use this command to enroll the local server to the specified trustpoint.  
Use the **no** variant of this command to de-enroll the server by removing its certificate

**Syntax** `crypto pki enroll <trustpoint>`  
`no crypto pki enroll <trustpoint>`

| Parameter                       | Description                               |
|---------------------------------|---|
| <code>&lt;trustpoint&gt;</code> | The name of the trustpoint to be enrolled |

**Mode** Privileged Exec

**Usage notes** For the local server, “enrollment” is the process of creating of a certificate for the server that has been signed by a CA associated with the trustpoint. The public portion of the RSA key pair specified using the `rsa` parameter for the trustpoint will be included in the server certificate.

If the trustpoint represents a locally self-signed certificate authority, then this command results in the direct generation of the server certificate, signed by the root CA for the trustpoint.

If the trustpoint represents an external certificate authority, then this command results in the generation of a Certificate Signing Request (CSR) file, which is displayed at the terminal in Privacy-Enhanced Mail (PEM) format, suitable for copying and pasting into a file or message. The CSR must be sent to the external CA for processing. When the CA replies with the signed certificate, that certificate should be imported using the `crypto pki import pem` command, to complete the enrollment process.

The specified trustpoint must already exist, and it must already be authenticated.

**Example** To enroll the local server with the trustpoint “example”, use the following commands:

```
awplus> enable
awplus# crypto pki enroll example
```

**Related commands** [crypto pki import pem](#)  
[crypto pki trustpoint](#)  
[enrollment \(ca-trustpoint\)](#)

# crypto pki export pem

**Overview** Use this command to export the root CA certificate for the given trustpoint to a file in Privacy-Enhanced Mail (PEM) format. The file may be transferred to the specified destination URL, or displayed at the terminal.

**Syntax** `crypto pki export <trustpoint> pem [terminal|<url>]`

| Parameter    | Description   |
|--------------|---|
| <trustpoint> | The name of the trustpoint for which the root CA certificate is to be exported. |
| terminal     | Display the PEM file to the terminal.   |
| <url>        | Transfer the PEM file to the specified URL.                                     |

**Default** The PEM will be displayed to the terminal by default.

**Mode** Privileged Exec

**Usage notes** The specified trustpoint must already exist, and it must already be authenticated.

**Example** To display the PEM file for the trustpoint "example" to the terminal, use the following commands:

```
awplus> enable
awplus# crypto pki export example pem terminal
```

To export the PEM file "example.pem" for the trustpoint "example" to the URL "tftp://server\_a/", use the following commands:

```
awplus> enable
awplus# crypto pki export example pem
tftp://server_a/example.pem
```

**Related commands**

- [crypto pki authenticate](#)
- [crypto pki import pem](#)
- [crypto pki trustpoint](#)

# crypto pki export pkcs12

**Overview** Use this command to export a certificate and private key for an entity in a trustpoint to a file in PKCS#12 format at the specified URL. The private key is encrypted with a passphrase for security.

**Syntax** `crypto pki export <trustpoint> pkcs12 {ca|server} <url>`

| Parameter                       | Description   |
|---------------------------------|---|
| <code>&lt;trustpoint&gt;</code> | The name of the trustpoint for which the certificate and key are to be exported.  |
| <code>ca</code>                 | If this option is specified, the command exports the root CA certificate and corresponding key.                               |
| <code>server</code>             | If this option is specified, the command exports the server certificate and corresponding key.                                |
| <code>&lt;url&gt;</code>        | The destination URL for the PKCS#12 file. The format of the URL is the same as any valid destination for a file copy command. |

**Mode** Privileged Exec

**Usage notes** If the **ca** option is specified, this command exports the root CA certificate and the corresponding private key, if the trustpoint has been authenticated as a locally selfsigned CA. (If the trustpoint represents an external CA, then there is no private key on the system corresponding to the root CA certificate. Use the **crypto pki export pem** file to export the certificate by itself.) The command prompts for a passphrase to encrypt the private key.

If the **server** option is specified, this command exports the server certificate and the corresponding private key, if the server has been enrolled to the trustpoint. The command prompts for a passphrase to encrypt the private key.

The key and certificate must already exist.

**Example** To export the PKCS#12 file "example.pk12" for the trustpoint "example" to the URL "tftp://backup/", use the following commands:

```
awplus> enable
awplus# crypto pki export example pkcs12 ca
tftp://backup/example.pk12
```

**Related commands** [crypto pki export pem](#)  
[crypto pki import pkcs12](#)

# crypto pki import pem

**Overview** This command imports a certificate for the given trustpoint from a file in Privacy-Enhanced Mail (PEM) format. The file may be transferred from the specified destination URL, or entered at the terminal.

**Syntax** `crypto pki import <trustpoint> pem [terminal|<url>]`

| Parameter                       | Description  |
|---------------------------------|--|
| <code>&lt;trustpoint&gt;</code> | The name of the trustpoint for which the root CA certificate is to be imported.  |
| <code>terminal</code>           | Optional parameter, If specified, the command prompts the user to enter (or paste) the PEM file at the terminal. If parameter is specified terminal is assumed by default. |
| <code>&lt;url&gt;</code>        | Optional parameter, If specified, the PEM file is transferred from the specified URL   |

**Default** The PEM will be imported from the terminal by default.

**Mode** Privileged Exec

**Usage notes** The command is generally used for trustpoints representing external certificate authorities. It accepts root CA certificates, intermediate CA certificates, and server certificates. The system automatically detects the certificate type upon import.

Using this command to import root CA certificates at the terminal is identical to the functionality provided by the `crypto pki authenticate` command, for external certificate authorities. The imported certificate is validated to ensure it is a proper CA certificate.

Intermediate CA certificates are validated to ensure they are proper CA certificates, and that the issuer chain ends in a root CA certificate already installed for the trustpoint. If there is no root CA certificate for the trustpoint (i.e., if the trustpoint is unauthenticated) then intermediate CA certificates may not be imported.

Server certificates are validated to ensure that the issuer chain ends in a root CA certificate already installed for the trustpoint. If there is no root CA certificate for the trustpoint (i.e., if the trustpoint is unauthenticated) then server certificates may not be imported.

The specified trustpoint must already exist. If the imported certificate is self-signed, then no certificates may exist for the trustpoint. Otherwise, the issuer's certificate must already be present for the trustpoint.

**Example** To import the PEM file for the trustpoint "example" from the terminal, use the following commands:

```
awplus> enable
awplus# crypto pki import example pem
```



To import the PEM file for the trustpoint "example" from the URL "tftp://server\_a/", use the following commands:

```
awplus> enable  
  
awplus# crypto pki import example pem  
tftp://server_a/example.pem
```

**Related commands**

- [crypto pki authenticate](#)
- [crypto pki export pem](#)
- [crypto pki trustpoint](#)

# crypto pki import pkcs12

**Overview** This command imports a certificate and private key for an entity in a trustpoint from a file in PKCS#12 format at the specified URL. The command prompts for a passphrase to decrypt the private key within the file.

**Syntax** `crypto pki import <trustpoint> pkcs12 {ca|server} <url>`

| Parameter    | Description  |
|--------------|--|
| <trustpoint> | The name of the trustpoint for which the certificate and key are to be imported.   |
| ca           | If this option is specified, the command imports the root CA certificate and corresponding key.                          |
| server       | If this option is specified, the command imports the server certificate and corresponding key.                           |
| <url>        | The source URL for the PKCS#12 file. The format of the URL is the same as any valid destination for a file copy command. |

**Mode** Privileged Exec

**Usage notes** If the **ca** option is specified, this command imports the root CA certificate and the corresponding private key. This is only valid if the root CA certificate does not already exist for the trustpoint (i.e., if the trustpoint is unauthenticated).

If the **server** option is specified, this command imports the server certificate and the corresponding private key. The imported private key is given a new unique label of the form "localN", where N is a non-negative integer. This operation is only valid if the server certificate does not already exist for the trustpoint (i.e., if the server is not enrolled to the trustpoint).

The specified trustpoint must already exist. The key and certificate must not already exist.

**Example** To import the PKCS#12 file "example.pk12" for the trustpoint "example" to the URL "tftp://backup/", use the following commands:

```
awplus> enable
awplus# crypto pki import example pkcs12 ca
tftp://backup/example.pk12
```

**Related commands** [crypto pki export pkcs12](#)  
[crypto pki import pem](#)

# crypto pki trustpoint

**Overview** Use this command to declare the named trustpoint and enter trustpoint configuration mode.

Use the **no** variant of this command to destroy the trustpoint.

**Syntax** `crypto pki trustpoint <trustpoint>`  
`no crypto pki trustpoint <trustpoint>`

| Parameter                       | Description   |
|---------------------------------|---|
| <code>&lt;trustpoint&gt;</code> | The name of the trustpoint. The name must start with an alphanumeric character, and may only contain alphanumeric characters, underscores, dashes, or periods. The maximum length of the name is 63 characters. |

**Mode** Global Configuration

**Usage notes** If the trustpoint did not previously exist, it is created as a new trustpoint. The trustpoint will be empty (unauthenticated) unless the name "local" is selected, in which case the system will automatically authenticate the trustpoint as a local self-signed certificate authority.

The **no** variant of this command destroys the trustpoint by removing all CA and server certificates associated with the trustpoint, as well as the private key associated with the root certificate (if the root certificate was locally self-signed). This is a destructive and irreversible operation, so this command should be used with caution.

**Example** To configure a trustpoint named "example", use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
```

**Related commands** [show crypto pki certificates](#)  
[show crypto pki trustpoint](#)

**Command changes** Version 5.4.6-1.1: command added to x930 Series  
Version 5.4.8-1: command added to x220, XS900MX, x550 Series  
Version 5.4.8-2.1: command added to SBx908 GEN2, x950 Series

# enrollment (ca-trustpoint)

**Overview** Use this command to declare how certificates will be added to the system for the current trustpoint.

**Syntax** `enrollment {selfsigned|terminal}`

| Parameter               | Description  |
|-------------------------|--|
| <code>selfsigned</code> | Sets the enrollment mode for the current trustpoint to selfsigned. |
| <code>terminal</code>   | Sets the enrollment mode for the current trustpoint to terminal.   |

**Mode** Trustpoint Configuration

**Usage notes** If the enrollment is set to **selfsigned**, then the system will generate a root CA certificate and its associated key when the **crypto pki authenticate** command is issued. It will generate a server certificate (signed by the root CA certificate) when the **crypto pki enroll** command is issued.

If the enrollment is set to **terminal**, then the system will prompt the user to paste the root CA certificate Privacy Enhanced Mail (PEM) file at the terminal, when the **crypto pki authenticate** command is issued. It will create a Certificate Signing Request (CSR) file for the local server when the **crypto pki enroll** command is issued. The server certificate received from the external CA should be imported using the **crypto pki import pem** command.

The trustpoint named "local" may only use the **selfsigned** enrollment setting.

If no enrollment mode is specified, the **crypto pki authenticate** command will fail for the trustpoint.

**Example** To configure the trustpoint named "example" and set its enrollment to **selfsigned**, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# enrollment selfsigned
```

**Related commands** [crypto pki enroll](#)

# fingerprint (ca-trustpoint)

**Overview** Use this command to declare that certificates with the specified fingerprint should be automatically accepted, when importing certificates from an external certificate authority. This can affect the behavior of the **crypto pki authenticate** and **crypto pki import pem** commands.

Use the **no** variant of this command to remove the specified fingerprint from the pre-accepted list.

**Syntax** fingerprint <word>  
no fingerprint <word>

| Parameter | Description   |
|-----------|---|
| <word>    | The fingerprint as a series of 40 hexadecimal characters, optionally separated into multiple character strings. |

**Default** By default, no fingerprints are pre-accepted for the trustpoint.

**Mode** Trustpoint Configuration

**Usage notes** Specifying a fingerprint adds it to a list of pre-accepted fingerprints for the trustpoint. When a certificate is imported, if it matches any of the pre-accepted values, then it will be saved in the system automatically. If the imported certificate's fingerprint does not match any pre-accepted value, then the user will be prompted to verify the certificate contents and fingerprint visually.

This command is useful when certificates from an external certificate authority are being transmitted over an insecure channel. If the certificate fingerprint is delivered via a separate messaging channel, then pre-entering the fingerprint value via cut-and-paste may be less errorprone than attempting to verify the fingerprint value visually.

The fingerprint is a series of 40 hexadecimal characters. It may be entered as a continuous string, or as a series of up to multiple strings separated by spaces. The input format is flexible because different certificate authorities may provide the fingerprint string in different formats.

**Example** To configure a fingerprint "5A81D34C 759CC4DA CFCA9F65 0303AD83 410B03AF" for the trustpoint named "example", use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# fingerprint 5A81D34C 759CC4DA CFCA9F65
0303AD83 410B03AF
```

**Related commands** [crypto pki authenticate](#)

`crypto pki import pem`

# no crypto pki certificate

**Overview** Use this command to delete a certificate with the specified fingerprint from the specified trustpoint.

**Syntax** `no crypto pki certificate <trustpoint> <word>`

| Parameter                       | Description   |
|---------------------------------|---|
| <code>&lt;trustpoint&gt;</code> | The name of the trustpoint.   |
| <code>&lt;word&gt;</code>       | The fingerprint as a series of 40 hexadecimal characters, optionally separated into multiple character strings. |

**Default** By default, no fingerprints are pre-accepted for the trustpoint.

**Mode** Privileged Exec

**Usage notes** The fingerprint can be found in the output of the **show crypto pki certificates** command. If there are dependent certificates in the trustpoint (i.e., if other certificates were signed by the specified certificate), the command will be rejected. If the specified certificate is the root CA certificate and the trustpoint represents a locally selfsigned CA, then the corresponding private key is also deleted from the system. Deleting the root CA certificate effectively resets the trustpoint to an unauthenticated state.

**Example** To delete a certificate with the fingerprint "594EDEF9 C7C4308C 36D408E0 77E784F0 A59E8792" from the trustpoint "example", use the following commands:

```
awplus> enable
awplus# no crypto pki certificate example
594EDEF9 C7C4308C 36D408E0 77E784F0 A59E8792
```

**Related commands** [no crypto pki trustpoint](#)  
[show crypto pki certificates](#)

# rsakeypair (ca-trustpoint)

**Overview** Use this command to declare which RSA key pair should be used to enroll the local server with the trustpoint. Note that this defines the key pair used with the server certificate, not the key pair used with the root CA certificate.

Use the **no** variant of this command to restore the default value, "server-default".

**Syntax** `rsakeypair <keylabel> [<1024-4096>]`  
`no rsakeypair`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;keylabel&gt;</code>  | The key to be used with the server certificate for this trustpoint. The name must start with an alphanumeric character, and may only contain alphanumeric characters, underscores, dashes, or periods. The maximum length of the name is 63 characters. |
| <code>&lt;1024-4096&gt;</code> | The bit length for the key, to be used if the key is implicitly generated during server enrollment.   |

**Default** The default value for **keylabel** is "server-default".  
The default value for the key bit length is 2048.

**Mode** Trustpoint Configuration

**Usage notes** If the label specified does not refer to an existing key created by the **crypto key generate rsa** command, the key will be implicitly generated when the **crypto pki enroll** command is issued to generate the server certificate or the server certificate signing request. The optional numeric parameter defines the bit length for the key, and is only applicable for keys that are implicitly created during enrollment.

This command does not affect server certificates or server certificate signing requests that have already been generated. The trustpoint's server certificate is set to use whatever key pair was specified for the trustpoint at the time the **crypto pki enroll** command is issued.

The default key pair is "server-default". The default bit length is 2048 bits.

**Example** To configure trustpoint "example" to use the key pair "example-server-key" with a bit length of 2048, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# rsakeypair example-server-key 2048
```

**Related commands** [crypto key generate rsa](#)



# show crypto key mypubkey rsa

**Overview** Use this command to display information about the specified Rivest-Shamir-Adleman encryption key.

**Syntax** `show crypto key mypubkey rsa [<keylabel>]`

| Parameter  | Description                                    |
|------------|--|
| <keylabel> | The name of the key to be shown, if specified. |

**Default** By default, all keys will be shown.

**Mode** Privileged Exec

**Usage notes** If no key label is specified, information about all keys is shown. The command displays the bit length of the key, a key fingerprint (a hash of the key contents to help uniquely identify a key), and a list of trustpoints in which the server certificate is using the key.

The specified keys must exist.

**Example** To show all keys, use the following commands:

```
awplus> enable
awplus# show crypto key mypubkey rsa
```

**Output** Figure 18-1: Example output from **show crypto key mypubkey rsa**

```
awplus#show crypto key mypubkey rsa
-----
RSA Key Pair "example-server-key":
  Key size      : 2048 bits
  Fingerprint   : 1A605D73 C2274CB7 853886B3 1C802FC6 7CDE45FB
  Trustpoints   : example
-----
RSA Key Pair "server-default":
  Key size      : 2048 bits
  Fingerprint   : 34AC4D2D 5249A168 29D426A3 434FFC59 C4A19901
  Trustpoints   : local
```

**Related commands** [crypto key generate rsa](#)

# show crypto pki certificates

**Overview** Use this command to display information about existing certificates for the specified trustpoint.

**Syntax** `show crypto pki certificates [<trustpoint>]`

| Parameter                       | Description  |
|---------------------------------|--|
| <code>&lt;trustpoint&gt;</code> | The trustpoint for which the certificates are to be shown. |

**Default** By default, the certificates for all trustpoints are shown.

**Mode** Privileged Exec

**Usage notes** If no trustpoint is specified, certificates for all trustpoints are shown. The command displays the certificates organized into certificate chains. It starts with the server certificate and then displays its issuer, and continues up the issuer chain until the root CA certificate is reached.

For each certificate, the command displays the certificate type, the subject's distinguished name (the entity identified by the certificate), the issuer's distinguished name (the entity that signed the certificate), the validity dates for the certificate, and the fingerprint of the certificate. The fingerprint is a cryptographic hash of the certificate contents that uniquely identifies the certificate.

The specified trustpoints must already exist.

**Example** To show the certificates for the trustpoint "example", use the following command:

```
awplus> enable
awplus# show crypto pki certificates example
```

**Output** Figure 18-2: Example output from **show crypto pki certificates**

```
awplus>enable
awplus#show crypto pki certificates example
-----
Trustpoint "example" Certificate Chain
-----
Server certificate
  Subject      : /O=local/CN=local.loc.lc
  Issuer       : /C=NZ/CN=local_Signing_CA
  Valid From   : Nov 11 15:35:21 2015 GMT
  Valid To     : Aug 31 15:35:21 2018 GMT
  Fingerprint  : 5A81D34C 759CC4DA CFCA9F65 0303AD83 410B03AF
Intermediate CA certificate
  Subject      : /C=NZ/CN=example_Signing_CA
  Issuer       : /C=NZ/CN=example_Root_CA
  Valid From   : Sep 3 18:45:01 2015 GMT
  Valid To     : Oct 10 18:45:01 2020 GMT
  Fingerprint  : AE2D5850 9867D258 ABBEE95E 2E0E3D81 60714920
Imported root certificate
  Subject      : /C=NZ/CN=example_Root_CA
  Issuer       : /C=NZ/CN=example_Root_CA
  Valid From   : Jul 23 18:12:10 2015 GMT
  Valid To     : May 12 18:12:10 2025 GMT
  Fingerprint  : 594EDEF9 C7C4308C 36D408E0 77E784F0 A59E8792
```

**Related commands** [crypto pki trustpoint](#)

# show crypto pki trustpoint

**Overview** Use this command to display information about the specified trustpoint.

**Syntax** `show crypto pki trustpoint [<trustpoint>]`

| Parameter                       | Description                            |
|---------------------------------|--|
| <code>&lt;trustpoint&gt;</code> | The name of the trustpoint to be shown |

**Default** By default, all trustpoints are shown.

**Mode** Privileged Exec

**Usage notes** If no trustpoint is specified, information about all trustpoints is shown. The command displays the authentication status of the trustpoint, the fingerprint of the root CA certificate (if it exists), the enrollment status of the local server with the trustpoint, a list of any applications that are configured to use the trustpoint, and the trustpoint parameters that were configured from trustpoint-configuration mode.

The specified trustpoints must already exist.

**Example** To show the details of the trustpoint "example", use the following commands:

```
awplus> enable
awplus# show crypto pki trustpoint example
```

**Output** Figure 18-3: Example output from **show crypto pki trustpoint**

```
awplus> enable
awplus# show crypto pki trustpoint example
-----
Trustpoint "example"
  Type           : Self-signed certificate authority
  Root Certificate: 50C1856B EEC7555A 0F3A61F6 690D9463 67DF74D1
  Local Server   : The server is enrolled to this trustpoint.
  Server Key     : example-server-key
  Applications    : RADIUS

Authentication and Enrollment Parameters:
  Enrollment     : selfsigned
  RSA Key Pair   : example-server-key (2048 bits)
-----
```

**Related commands** [crypto pki trustpoint](#)  
[show crypto pki certificates](#)

# subject-name (ca-trustpoint)

**Overview** Use this command to specify the distinguished name string that should be used for the subject field in the server certificate, when enrolling the server (generating the server certificate or server certificate signing request).

**Syntax** `subject-name <word>`

| Parameter                 | Description   |
|---------------------------|---|
| <code>&lt;word&gt;</code> | Specify the subject name as a distinguished name string. Complex strings (e.g., strings containing spaces) should be surrounded with double-quote characters. |

**Default** If no subject name is specified for the trustpoint, then the system automatically builds a name of the form `/O=AlliedWare Plus/CN=xxxx.yyyy.zzz`, where `xxxx` is the hostname of the system and `yyyy.zzz` is the default search domain for the system.

**Mode** Trustpoint Configuration

**Usage notes** The subject name is specified as a variable number of fields, where each field begins with a forward-slash character (`/`). Each field is of the form `XX=value`, where `XX` is the abbreviation of the node type in the tree.

Common values include:

- `"C"` (country),
- `"ST"` (state),
- `"L"` (locality),
- `"O"` (organization),
- `"OU"` (organizational unit), and
- `"CN"` (common name).

Of these fields, `"CN"` is usually the most important.

**NOTE:** For a server certificate, many applications require that the network name of the server matches the common name in the server's certificate.

**Example** To configure the trustpoint named "example" and set its subject name, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# subject-name "/O=My
Company/CN=192.168.1.1
```

**Related  
commands** [crypto pki enroll](#)

# Part 5: Network Management

# 19

# Allied Telesis Management Framework™ (AMF) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for Allied Telesis Management Framework™ (AMF) commands.

**AMF master nodes** Every AMF network must have at least one master node, which acts as the core of the AMF network. Not all AlliedWare Plus devices are capable of acting as an AMF master. See the [AMF Feature Overview and Configuration Guide](#) for information about AMF master support.

**AMF edge** AlliedWare Plus CentreCOM® Series switches can only be used as edge switches in an AMF network. The full management power and convenience of AMF is available on these switches, but they can only link to one other AMF node. They cannot form cross-links or virtual links.

**AMF naming convention** When AMF is enabled on a device, it will automatically be assigned a host name. If a host name has already been assigned, by using the command [hostname](#) on page 184, this will remain. If however, no host name has been assigned, then the name applied will be the prefix, **host\_** followed (without a space) by the MAC address of the device. For example, a device whose MAC address is **0016.76b1.7a5e** will have the name **host\_0016\_76b1\_7a5e** assigned to it.

To efficiently manage your network using AMF, we strongly advise that you devise a naming convention for your network devices, and apply an appropriate hostname to each device in your AMF network.

**AMF and STP** On AR-Series UTM firewalls and Secure VPN routers, you cannot use STP at the same time as AMF.

- Command List**
- [“application-proxy ip-filter”](#) on page 653
  - [“application-proxy quarantine-vlan”](#) on page 654
  - [“application-proxy redirect-url”](#) on page 655
  - [“application-proxy threat-protection”](#) on page 656
  - [“application-proxy threat-protection send-summary”](#) on page 657



- [“application-proxy whitelist enable”](#) on page 658
- [“application-proxy whitelist server”](#) on page 659
- [“area-link”](#) on page 661
- [“atmf area”](#) on page 663
- [“atmf area password”](#) on page 665
- [“atmf authorize”](#) on page 667
- [“atmf authorize provision”](#) on page 669
- [“atmf backup”](#) on page 671
- [“atmf backup area-masters delete”](#) on page 672
- [“atmf backup area-masters enable”](#) on page 673
- [“atmf backup area-masters now”](#) on page 674
- [“atmf backup area-masters synchronize”](#) on page 675
- [“atmf backup bandwidth”](#) on page 676
- [“atmf backup delete”](#) on page 677
- [“atmf backup enable”](#) on page 678
- [“atmf backup guests delete”](#) on page 679
- [“atmf backup guests enable”](#) on page 680
- [“atmf backup guests now”](#) on page 681
- [“atmf backup guests synchronize”](#) on page 682
- [“atmf backup now”](#) on page 683
- [“atmf backup redundancy enable”](#) on page 685
- [“atmf backup server”](#) on page 686
- [“atmf backup stop”](#) on page 688
- [“atmf backup synchronize”](#) on page 689
- [“atmf cleanup”](#) on page 690
- [“atmf container”](#) on page 691
- [“atmf container login”](#) on page 692
- [“atmf controller”](#) on page 693
- [“atmf distribute firmware”](#) on page 694
- [“atmf domain vlan”](#) on page 696
- [“atmf enable”](#) on page 699
- [“atmf group \(membership\)”](#) on page 700
- [“atmf guest-class”](#) on page 702
- [“atmf log-verbose”](#) on page 704
- [“atmf management subnet”](#) on page 705

- [“atmf management vlan”](#) on page 708
- [“atmf master”](#) on page 710
- [“atmf mtu”](#) on page 711
- [“atmf network-name”](#) on page 712
- [“atmf provision \(interface\)”](#) on page 713
- [“atmf provision node”](#) on page 714
- [“atmf reboot-rolling”](#) on page 716
- [“atmf recover”](#) on page 720
- [“atmf recover guest”](#) on page 722
- [“atmf recover led-off”](#) on page 723
- [“atmf recovery-server”](#) on page 724
- [“atmf remote-login”](#) on page 726
- [“atmf restricted-login”](#) on page 728
- [“atmf secure-mode”](#) on page 730
- [“atmf secure-mode certificate expire”](#) on page 732
- [“atmf secure-mode certificate expiry”](#) on page 733
- [“atmf secure-mode certificate renew”](#) on page 734
- [“atmf secure-mode enable-all”](#) on page 735
- [“atmf select-area”](#) on page 737
- [“atmf topology-gui enable”](#) on page 738
- [“atmf trustpoint”](#) on page 739
- [“atmf virtual-crosslink”](#) on page 741
- [“atmf virtual-link”](#) on page 743
- [“atmf virtual-link protection”](#) on page 746
- [“atmf working-set”](#) on page 748
- [“bridge-group”](#) on page 750
- [“clear application-proxy threat-protection”](#) on page 751
- [“clear atmf links”](#) on page 752
- [“clear atmf links virtual”](#) on page 753
- [“clear atmf links statistics”](#) on page 754
- [“clear atmf recovery-file”](#) on page 755
- [“clear atmf secure-mode certificates”](#) on page 756
- [“clear atmf secure-mode statistics”](#) on page 757
- [“clone \(amf-provision\)”](#) on page 758
- [“configure boot config \(amf-provision\)”](#) on page 760

- [“configure boot system \(amf-provision\)”](#) on page 762
- [“copy \(amf-provision\)”](#) on page 764
- [“create \(amf-provision\)”](#) on page 765
- [“debug atmf”](#) on page 767
- [“debug atmf packet”](#) on page 769
- [“delete \(amf-provision\)”](#) on page 772
- [“discovery”](#) on page 774
- [“description \(amf-container\)”](#) on page 776
- [“erase factory-default”](#) on page 777
- [“http-enable”](#) on page 778
- [“identity \(amf-provision\)”](#) on page 780
- [“license-cert \(amf-provision\)”](#) on page 782
- [“locate \(amf-provision\)”](#) on page 784
- [“log event-host”](#) on page 786
- [“modeltype”](#) on page 787
- [“service atmf-application-proxy”](#) on page 788
- [“show application-proxy threat-protection”](#) on page 789
- [“show application-proxy whitelist interface”](#) on page 791
- [“show application-proxy whitelist server”](#) on page 793
- [“show application-proxy whitelist supplicant”](#) on page 794
- [“show atmf”](#) on page 796
- [“show atmf area”](#) on page 800
- [“show atmf area guests”](#) on page 803
- [“show atmf area guests-detail”](#) on page 805
- [“show atmf area nodes”](#) on page 807
- [“show atmf area nodes-detail”](#) on page 809
- [“show atmf area summary”](#) on page 811
- [“show atmf authorization”](#) on page 812
- [“show atmf backup”](#) on page 815
- [“show atmf backup area”](#) on page 819
- [“show atmf backup guest”](#) on page 821
- [“show atmf container”](#) on page 823
- [“show atmf detail”](#) on page 826
- [“show atmf group”](#) on page 828
- [“show atmf group members”](#) on page 830

- “show atmf guests” on page 832
- “show atmf guests detail” on page 834
- “show atmf links” on page 837
- “show atmf links detail” on page 839
- “show atmf links guest” on page 848
- “show atmf links guest detail” on page 850
- “show atmf links statistics” on page 854
- “show atmf nodes” on page 857
- “show atmf provision nodes” on page 859
- “show atmf recovery-file” on page 861
- “show atmf secure-mode” on page 862
- “show atmf secure-mode audit” on page 864
- “show atmf secure-mode audit link” on page 865
- “show atmf secure-mode certificates” on page 866
- “show atmf secure-mode sa” on page 869
- “show atmf secure-mode statistics” on page 872
- “show atmf tech” on page 874
- “show atmf virtual-links” on page 877
- “show atmf working-set” on page 879
- “show debugging atmf” on page 880
- “show debugging atmf packet” on page 881
- “show running-config atmf” on page 882
- “state” on page 883
- “switchport atmf-agentlink” on page 885
- “switchport atmf-arealink remote-area” on page 886
- “switchport atmf-crosslink” on page 888
- “switchport atmf-guestlink” on page 890
- “switchport atmf-link” on page 892
- “type atmf node” on page 893
- “undebg atmf” on page 896
- “username” on page 897

# application-proxy ip-filter

**Overview** Use this command to enable global IP filtering on a device. Once enabled the device will add a global ACL in response to a threat message from an AMF Security (AMF-Sec) Controller.

Use the **no** variant of this command to disable global IP filtering.

**Syntax** `application-proxy ip-filter`  
`no application-proxy ip-filter`

**Default** Global IP filtering is disabled by default.

**Mode** Global Configuration

**Usage notes** For this feature to work, the AMF Application Proxy service needs to be enabled on your network, using the command [service atmf-application-proxy](#).

**Example** To enable global IP filtering, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy ip-filter
```

To disable global IP filtering, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy ip-filter
```

**Related commands** [application-proxy redirect-url](#)  
[application-proxy threat-protection](#)  
[clear application-proxy threat-protection](#)  
[service atmf-application-proxy](#)  
[show application-proxy threat-protection](#)

**Command changes** Version 5.4.7-2.5: command added

# application-proxy quarantine-vlan

**Overview** Use this command to set the quarantine VLAN to use when an AMF Security (AMF-Sec) Controller detects a threat. The port/s on which the threat is detected are moved to this VLAN if the [application-proxy threat-protection](#) action is set to **quarantine**.

Use the **no** variant of this command to delete the quarantine VLAN. If no quarantine VLAN is specified then no quarantine action will be performed.

**Syntax** `application-proxy quarantine-vlan <vlan-id>`  
`no application-proxy quarantine-vlan`

| Parameter                    | Description                                     |
|------------------------------|---|
| <code>&lt;vlan-id&gt;</code> | The ID of the VLAN to use. In the range 1-4094. |

**Default** By default, no quarantine VLAN is configured.

**Mode** Global Configuration

**Example** To configure VLAN 100 as the quarantine VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy quarantine-vlan 100
```

To delete the quarantine VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy quarantine-vlan
```

**Related commands** [application-proxy threat-protection](#)  
[clear application-proxy threat-protection](#)  
[application-proxy threat-protection send-summary](#)  
[service atmf-application-proxy](#)  
[show application-proxy threat-protection](#)

**Command changes** Version 5.4.7-2.2: command added

# application-proxy redirect-url

**Overview** Use this command to redirect a user to a helpful URL when they are blocked because of an [application-proxy ip-filter](#).

Use the **no** variant of this command to remove the URL redirect.

**Syntax** `application-proxy redirect-url <url>`  
`no application-proxy redirect-url`

| Parameter                | Description                  |
|--------------------------|------------------------------|
| <code>&lt;url&gt;</code> | URL to redirect the user to. |

**Default** No URL is configured by default.

**Mode** Global Configuration

**Example** To configure a redirect URL, use the command:

```
awplus# application-proxy redirect-url http://my.dom/help.html
```

To remove a redirect URL, use the command:

```
awplus# no application-proxy redirect-url
```

**Related commands** [application-proxy ip-filter](#)  
[application-proxy threat-protection](#)  
[clear application-proxy threat-protection](#)  
[service atmf-application-proxy](#)  
[show application-proxy threat-protection](#)

**Command changes** Version 5.4.9-0.1: command added

# application-proxy threat-protection

**Overview** Use this command to set the blocking action to take when a threat detected message is received from an AMF Security (AMF-Sec) Controller.

Use the **no** variant of this command to disable threat protection blocking actions on the port.

**Syntax** application-proxy threat-protection {drop|link-down|  
quarantine|log-only}  
no application-proxy threat-protection

| Parameter  | Description   |
|------------|---|
| drop       | Apply a Layer 2 drop for traffic generating the threat reports. |
| link-down  | Set the link to error disabled in response to threats.          |
| quarantine | Move the offending port to a quarantine VLAN.                   |
| log-only   | Log when a threat is detected.                                  |

**Default** Threat protection is disabled by default.

**Mode** Interface Configuration

**Example** To set the threat protection blocking action on port1.0.4 to drop, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# application-proxy threat-protection drop
```

To disable threat protection blocking actions on port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no application-proxy threat-protection
```

**Related commands** [application-proxy quarantine-vlan](#)  
[application-proxy threat-protection send-summary](#)  
[clear application-proxy threat-protection](#)  
[service atmf-application-proxy](#)  
[show application-proxy threat-protection](#)

**Command changes** Version 5.4.7-2.2: command added  
Version 5.4.9-0.1: **log-only** parameter added



# application-proxy threat-protection send-summary

**Overview** Use this command to send a summary of all current threat-protection blocking requests to all AMF Application Proxy service nodes. This command can only be performed on an AMF master.

**Syntax** `application-proxy threat-protection send-summary`

**Mode** Privileged Exec

**Example** To send a summary of all current threat-protection blocking requests to all AMF Application Proxy service nodes, use the command:

```
awplus# application-proxy threat-protection send-summary
```

**Related commands**

- [application-proxy quarantine-vlan](#)
- [application-proxy threat-protection](#)
- [clear application-proxy threat-protection](#)
- [service atmf-application-proxy](#)
- [show application-proxy threat-protection](#)

**Command changes** Version 5.4.7-2.2: command added

# application-proxy whitelist enable

**Overview** Use this command to enable application-proxy whitelist based authentication on an interface.

Use the **no** variant of this command to disable the whitelist authentication.

**Syntax** application-proxy whitelist enable  
no application-proxy whitelist enable

**Default** Application-proxy whitelist is disabled by default.

**Mode** Interface Configuration

**Example** To enable application-proxy whitelist authentication on the interface port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# application-proxy whitelist enable
```

To disable application-proxy whitelist authentication on the interface port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no application-proxy whitelist enable
```

**Related commands** application-proxy whitelist server  
show application-proxy whitelist interface  
show application-proxy whitelist server  
show application-proxy whitelist supplicant

**Command changes** Version 5.4.9-0.1: command added

# application-proxy whitelist server

**Overview** Use this command to set an AMF master to act as a whitelist authentication proxy between AMF members, acting as Network Access Servers, and an external whitelist RADIUS server.

Use the **no** variant of this command to disable the whitelist proxy functionality.

**Syntax** `application-proxy whitelist server <ip-address> key <key>`  
`[auth-port <1-65535>]`  
`no application-proxy whitelist server`

| Parameter                              | Description  |
|--|--|
| <code>&lt;ip-address&gt;</code>        | IPv4 address of the upstream RADIUS server in dotted decimal format A.B.C.D.                           |
| <code>key &lt;key&gt;</code>           | Set the shared secret encryption key for communication with the upstream RADIUS server.                |
| <code>auth-port &lt;1-65535&gt;</code> | Set the RADIUS server UDP port. This is only necessary if you don't want to use the default port 1812. |

**Default** Disabled by default.

**Mode** Global Configuration

**Example** To configure an AMF master to work as a proxy to the external RADIUS server 192.168.1.10, with shared secret 'mysecurekey', on port 1822, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist server 192.168.1.10
key mysecurekey auth-port 1822
```

To configure an AMF master to work as a proxy to the external RADIUS server 192.168.1.10, with shared secret 'mysecurekey', on the default port (1812), use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist server 192.168.1.10
key mysecurekey
```

To disable the whitelist proxy, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy whitelist server
```

**Related commands**

- [application-proxy whitelist enable](#)
- [service atmf-application-proxy](#)
- [show application-proxy whitelist interface](#)
- [show application-proxy whitelist server](#)

show application-proxy whitelist supplicant

**Command changes** Version 5.4.9-0.1: command added

# area-link

**Overview** Use this command to create an area-link between a Virtual AMF Appliance (VAA) host controller and an AMF container.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove an area-link from a container.

**Syntax** `area-link <area-name>`  
`no area-link`

| Parameter                      | Description                            |
|--------------------------------|--|
| <code>&lt;area-name&gt;</code> | AMF area name of the container's area. |

**Mode** AMF Container Configuration

**Usage notes** The AMF area-link connects the AMF controller on a VAA host to the AMF container. Once a container has been created with the [atmf container](#) command and an area-link configured with the **area-link** command, it can be enabled using the [state](#) command.

You can only configure a single area-link on a container. You will see the following message if you try and configure a second one:

```
% AreaLink already configured for this container
```

Each container has two virtual interfaces:

- Interface eth0, used to connect to the AMF controller on the VAA host via an AMF area-link, configured using this area-link command.
- Interface eth1, used to connect to the outside world using a bridged L2 network link, configured using the [bridge-group](#) command.

See the [AMF Feature Overview and Configuration\\_Guide](#) for more information on these virtual interfaces and links.

**Example** To create the area-link to "wlg" on container "vac-wlg-1", use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# area-link wlg
```

To remove an area-link from container “vac-wlg-1”, use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# no area-link
```

**Related  
commands**

[atmf container](#)  
[show atmf container](#)

**Command  
changes**

Version 5.4.7-0.1: command added

# atmf area

**Overview** This command creates an AMF area and gives it a name and ID number. Use the **no** variant of this command to remove the AMF area. This command is only valid on AMF controllers, master nodes and gateway nodes.

**Syntax** `atmf area <area-name> id <1-126> [local]`  
`no atmf area <area-name>`

| Parameter   | Description   |
|-------------|---|
| <area-name> | The AMF area name. The area name can be up to 15 characters long. Valid characters are:<br>a..z<br>A..Z<br>0..9<br>-<br>_ Names are case sensitive and must be unique within an AMF network. The name cannot be the word "local" or an abbreviation of the word "local" (such as "l", "lo" etc.). |
| <1-126>     | An ID number that uniquely identifies this area.  |
| local       | Set the area to be the local area. The local area contains the device you are configuring.  |

**Mode** Global Configuration

**Usage notes** This command enables you to divide your AMF network into areas. Each area is managed by at least one AMF master node. Each area can have up to 120 nodes, depending on the license installed on that area's master node.

The whole AMF network is managed by up to 8 AMF controllers. Each AMF controller can communicate with multiple areas. The number of areas supported on a controller depends on the license installed on that controller.

You must give each area in an AMF network a unique name and ID number.

Only one local area can be configured on a device. You must specify a local area on each controller, remote AMF master, and gateway node.

**Example** To create the AMF area named *New-Zealand*, with an ID of 1, and specify that it is the local area, use the command:

```
controller-1(config)# atmf area New-Zealand id 1 local
```

To configure a remote area named *Auckland*, with an ID of 100, use the command:

```
controller-1(config)# atmf area Auckland id 100
```

**Related commands**

- atmf area password
- show atmf area
- show atmf area summary
- show atmf area nodes
- switchport atmf-arealink remote-area



# atmf area password

**Overview** This command sets a password on an AMF area.

Use the **no** variant of this command to remove the password.

This command is only valid on AMF controllers, master nodes and gateway nodes. The area name must have been configured first.

**Syntax** `atmf area <area-name> password [8] <password>`  
`no atmf area <area-name> password`

| Parameter   | Description   |
|-------------|---|
| <area-name> | The AMF area name.  |
| 8           | This parameter is displayed in <b>show running-config</b> output to indicate that it is displaying the password in encrypted form. You should not enter <b>8</b> on the CLI yourself. |
| <password>  | The password is between 8 and 32 characters long. It can include spaces.  |

**Mode** Global Configuration

**Usage notes** You must configure a password on each area that an AMF controller communicates with, except for the controller's local area. The areas must already have been created using the `atmf area` command.

Enter the password identically on both of:

- the area that locally contains the controller, and
- the remote AMF area masters

The command **show running-config atmf** will display the encrypted version of this password. The encryption keys will match between the controller and the remote AMF master.

If multiple controller and masters exist in an area, they must all have the same area configuration.

**Example** To give the AMF area named *Auckland* a password of "secure#1" use the following command on the controller:

```
controller-1(config)# atmf area Auckland password secure#1
```

and also use the following command on the master node for the Auckland area:

```
auck-master(config)# atmf area Auckland password secure#1
```

**Related commands**

- atmf area
- show atmf area
- show atmf area summary
- show atmf area nodes
- switchport atmf-arealink remote-area

# atmf authorize

**Overview** On an AMF network, with secure mode enabled, use this command on an AMF master to authorize an AMF node to join the network. AMF nodes waiting to be authorized appear in the pending authorization queue, which can be examined using the [show atmf authorization](#) command with the **pending** parameter.

Use the **no** variant of this command to revoke authorization for an AMF node on an AMF master.

**Syntax** `atmf authorize {<node-name> [area <area-name>]|all-pending}`  
`no atmf authorize <node-name> [area <area-name>]`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;node-name&gt;</code> | The name of the node to be authorized or have its authorization revoked. |
| <code>area</code>              | Specify an AMF area.   |
| <code>&lt;area-name&gt;</code> | This is the name of the area the node belongs to.                        |
| <code>all-pending</code>       | Authorize all nodes in the pending queue.                                |

**Mode** Privileged Exec

**Usage notes** On an AMF controller, AMF remote-area masters must be authorized by the controller, and the AMF remote-area masters will also need to authorized access from the AMF controller.

**Example** To authorize all AMF nodes in the pending authorization queue on an AMF master, use the command:

```
awplus# atmf authorize all-pending
```

To authorize a node called "node2" in remote AMF area "area3", use the command:

```
awplus# atmf authorize node2 area "area3"
```

To authorize a node called "node4" on an AMF master, use the command:

```
awplus# atmf authorize node4
```

To revoke authorization for a node called "node4" on an AMF master, use the command:

```
awplus# no atmf authorize node4
```

**Related commands**

- [atmf secure-mode](#)
- [clear atmf secure-mode certificates](#)
- [show atmf authorization](#)
- [show atmf secure-mode](#)

show atmf secure-mode certificates

show atmf secure-mode statistics

**Command changes** Version 5.4.7-0.3: command added

# atmf authorize provision

**Overview** Use this command from an AMF controller or AMF master to pre-authorize a node on an AMF network running in secure mode. This allows a node to join the AMF network the moment the `atmf secure-mode` command is run on that node.

Use the **no** variant of this command to remove a provisional authorization from and AMF controller or AMF master.

**Syntax**

```
atmf authorize provision [timeout <minutes>] node <node-name>
interface <interface-name> [area <area-name>]

atmf authorize provision [timeout <minutes>] mac <mac-address>

atmf authorize provision [timeout <minutes>] all

no atmf authorize provision node <node-name> interface
<interface-name> [area <area-name>]

no atmf authorize provision mac <mac-address>

no atmf authorize provision all
```

| Parameter        | Description  |
|------------------|--|
| timeout          | Timeout for provisional authorization. Authorization for provisioned nodes expires after the timeout period specified. |
| <minutes>        | Timeout in minutes. A value between 1 and 6000 is permissible with the default being 60 minutes.                       |
| node             | Specify a node to provision by node name.  |
| <node-name>      | The name of the node to provisionally authorize.   |
| interface        | Specify the interface the node will connect on.  |
| <interface-name> | The name of the interface, this can be a switchport, link aggregator, LACP link, or virtual link.                      |
| area             | Specify the AMF area.  |
| <area-name>      | This is the name of the area the node belongs to.  |
| mac              | Specify a node to provision by MAC address.  |
| <mac-address>    | Enter a MAC address to provisionally authorize in the format HHHH.HHHH.HHHH.   |
| all              | Provision authorization for all secure mode capable nodes.   |

**Default** The default timeout is 60 minutes.

**Mode** Privileged Exec

**Example** To provisionally authorize all non-secure AMF nodes, use the command:

```
awplus# atmf authorize provision all
```

To authorize a node with a MAC address of 0000.cd28.0880 for 2 hours, use the command:

```
awplus# authorize provision timeout 120 mac 0000.cd28.0880
```

To remove all provisional authorization, on an AMF master, use the command:

```
awplus# no atmf authorize provision all
```

**Related commands** [show atmf authorization](#)  
[show atmf secure-mode](#)

**Command changes** Version 5.4.7-0.3: command added

# atmf backup

**Overview** This command can only be applied to a master node. It manually schedules an AMF backup to start at a specified time and to execute a specified number of times per day.

Use the **no** variant of this command to disable the schedule.

**Syntax** `atmf backup {default|<hh:mm> frequency <1-24>}`

| Parameter        | Description  |
|------------------|--|
| default          | Restore the default backup schedule.   |
| <hh:mm>          | Sets the time of day to apply the first backup, in hours and minutes. Note that this parameter uses the 24 hour clock. |
| backup           | Enables AMF backup to external media.  |
| frequency <1-24> | Sets the number of times within a 24 hour period that backups will be taken.   |

**Default** Backups run daily at 03:00 AM, by default

**Mode** Global Configuration

**Usage notes** Running this command only configures the schedule. To enable the schedule, you should then apply the command [atmf backup enable](#).

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

**Example** To schedule backup requests to begin at 11 am and execute twice per day (11 am and 11 pm), use the following command:

```
node_1# configure terminal
node_1(config)# atmf backup 11:00 frequency 2
```

**CAUTION:** File names that comprise identical text, but with differing case, such as *Test.txt* and *test.txt*, will not be recognized as being different on FAT32 based backup media such as a USB storage device. However, these filenames will be recognized as being different on your Linux based device. Therefore, for good practice, ensure that you apply a consistent case structure for your back-up file names.

**Related commands** [atmf backup enable](#)  
[atmf backup stop](#)  
[show atmf backup](#)

# atmf backup area-masters delete

**Overview** Use this command to delete from external media, a backup of a specified node in a specified area.

Note that this command can only be run on an AMF controller.

**Syntax** `atmf backup area-masters delete area <area-name> node <node-name>`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;area-name&gt;</code> | The area that contains the node whose backup will be deleted. |
| <code>&lt;node-name&gt;</code> | The node whose backup will be deleted.                        |

**Mode** Privileged Exec

**Example** To delete the backup of the remote area-master named “well-gate” in the AMF area named Wellington, use the command:

```
controller-1# atmf backup area-masters delete area Wellington  
node well-gate
```

**Related commands** [show atmf backup area](#)



# atmf backup area-masters enable

**Overview** Use this command to enable backup of remote area-masters from the AMF controller. This command is only valid on AMF controllers.

Use the **no** form of the command to stop backups of remote area-masters.

**Syntax** `atmf backup area-masters enable`  
`no atmf backup area-masters enable`

**Mode** Global configuration

**Default** Remote area backups are disabled by default

**Usage notes** Use the following commands to configure the remote area-master backups:

- [atmf backup](#) to configure when the backups begin and how often they run
- [atmf backup server](#) to configure the backup server.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

**Example** To enable scheduled backups of AMF remote area-masters, use the commands:

```
controller-1# configure terminal
controller-1(config)# atmf backup area-masters enable
```

To disable scheduled backups of AMF remote area-masters, use the commands:

```
controller-1# configure terminal
controller-1(config)# no atmf backup area-masters enable
```

**Related commands** [atmf backup server](#)  
[atmf backup](#)  
[show atmf backup area](#)

# atmf backup area-masters now

**Overview** Use this command to run an AMF backup of one or more remote area-masters from the AMF controller immediately.

This command is only valid on AMF controllers.

**Syntax** `atmf backup area-masters now [area <area-name> | area <area-name> node <node-name>]`

| Parameter   | Description                                    |
|-------------|--|
| <area-name> | The area whose area-masters will be backed up. |
| <node-name> | The node that will be backed up.               |

**Mode** Privileged Exec

**Example** To back up all local master nodes in all areas controlled by controller-1, use the command

```
controller-1# atmf backup area-masters now
```

To back up all local masters in the AMF area named Wellington, use the command

```
controller-1# atmf backup area-masters now area Wellington
```

To back up the local master "well-master" in the Wellington area, use the command

```
controller-1# atmf backup area-masters now area Wellington node well-master
```

**Related commands** [atmf backup area-masters enable](#)  
[atmf backup area-masters synchronize](#)  
[show atmf backup area](#)

# atmf backup area-masters synchronize

**Overview** Use this command to synchronize backed-up area-master files between the active remote file server and the backup remote file server. Files are copied from the active server to the remote server.

Note that this command is only valid on AMF controllers.

**Syntax** `atmf backup area-masters synchronize`

**Mode** Privileged Exec

**Example** To synchronize backed-up files between the remote file servers for all area-masters, use the command:

```
controller-1# atmf backup area-masters synchronize
```

**Related commands**

- [atmf backup area-masters enable](#)
- [atmf backup area-masters now](#)
- [show atmf backup area](#)

# atmf backup bandwidth

**Overview** This command sets the maximum bandwidth in kilobytes per second (kBps) available to the AMF backup process. This command enables you to restrict the bandwidth that is utilized for downloading file contents during a backup.

**NOTE:** *This command will only run on an AMF master. An error message will be generated if the command is attempted on node that is not a master.*

*Also note that setting the bandwidth value to zero will allow the transmission of as much bandwidth as is available, which can exceed the maximum configurable speed of 1000 kBps. In effect, zero means unlimited.*

Use the **no** variant of this command to reset (to its default value of zero) the maximum bandwidth in kilobytes per second (kBps) available when initiating an AMF backup. A value of zero tells the backup process to transfer files using unlimited bandwidth.

**Syntax** `atmf backup bandwidth <0-1000>`  
`no atmf backup bandwidth`

| Parameter                   | Description                                       |
|-----------------------------|---|
| <code>&lt;0-1000&gt;</code> | Sets the bandwidth in kilobytes per second (kBps) |

**Default** The default value is zero, allowing unlimited bandwidth when executing an AMF backup.

**Mode** Global Configuration

**Examples** To set an atmf backup bandwidth of 750 kBps, use the commands:

```
node2# configure terminal
node2(config)# atmf backup bandwidth 750
```

To set the AMF backup bandwidth to the default value for unlimited bandwidth, use the commands:

```
node2# configure terminal
node2(config)# no atmf backup bandwidth
```

**Related commands** [show atmf backup](#)

# atmf backup delete

**Overview** This command removes the backup file from the external media of a specified AMF node.

Note that this command can only be run from an AMF master node.

**Syntax** `atmf backup delete <node-name>`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;node-name&gt;</code> | The AMF node name of the backup file to be deleted. |

**Mode** Privileged Exec

**Example** To delete the backup file from node2, use the following command:

```
Node_1# atmf backup delete node2
```

**Related commands**

- `show atmf backup`
- `atmf backup now`
- `atmf backup stop`

# atmf backup enable

**Overview** This command enables automatic AMF backups on the AMF master node that you are connected to. By default, automatic backup starts at 3:00 AM. However, this schedule can be changed by the [atmf backup](#) command. Note that backups are initiated and stored only on the master nodes.

Use the **no** variant of this command to disable any AMF backups that have been scheduled and previously enabled.

**Syntax** `atmf backup enable`  
`no atmf backup enable`

**Default** Automatic AMF backup functionality is enabled on the AMF master when it is configured and external media, i.e. an SD card or a USB storage device or remote server, is detected.

**Mode** Global Configuration

**Usage notes** A warning message will appear if you run the [atmf backup enable](#) command with either insufficient or marginal memory availability on your external storage device.

You can use the command [show atmf backup](#) on page 815 to check the amount of space available on your external storage device.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

**Example** To turn on automatic AMF backup, use the following command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup enable
```

**Related commands** [show atmf](#)  
[show atmf backup](#)  
[atmf backup](#)  
[atmf backup now](#)  
[atmf enable](#)

# atmf backup guests delete

**Overview** This command removes a guest node's backup files from external media such as a USB drive, SD card, or an external file server.

**Syntax** `atmf backup guests delete <node-name> <guest-port>`

| Parameter                       | Description                          |
|---------------------------------|--------------------------------------|
| <code>&lt;node-name&gt;</code>  | The name of the guest's parent node. |
| <code>&lt;guest-port&gt;</code> | The port number on the parent node.  |

**Mode** User Exec/Privileged Exec

**Example** On a parent node named "node1" (which, in this case, the user has a direct console connection to) use the following command to remove the backup files of the guest node that is directly connected to port1.0.3.

```
node1# atmf backup guests delete node1 port1.0.3
```

**Related Command**

- [atmf backup delete](#)
- [atmf backup area-masters delete](#)
- [show atmf backup guest](#)

# atmf backup guests enable

**Overview** Use this command to enable backups of remote guest nodes from an AMF master. Use the **no** variant of this command to disable the ability of the guest nodes to be backed up.

**Syntax** `atmf backup guests enable`  
`no atmf backup guests enable`

**Default** Guest node backups are enabled by default.

**Mode** Global Config

**Usage notes** We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

**Example** On the AMF master node, enable all scheduled guest node backups:

```
atmf-master# configure terminal
atmf-master(config)# atmf backup guests enable
```

**Related commands** `atmf backup area-masters enable`  
`show atmf backup guest`  
`atmf backup guests synchronize`



# atmf backup guests now

**Overview** This command manually triggers an AMF backup of guest nodes on a AMF Master.

**Syntax** `atmf backup guests now [<node-name>] [<guest-port>]`

| Parameter                       | Description                                      |
|---------------------------------|--|
| <code>&lt;node-name&gt;</code>  | The name of the guest's parent node.             |
| <code>&lt;guest-port&gt;</code> | The port number that connects to the guest node. |

**Default** n/a

**Mode** Privileged Exec

**Example** Use the following command to manually trigger the backup of all guests in the AMF network

```
awplus# atmf backup guests now
```

**Example** To manually trigger the backup of a guest node connected to port 1.0.23 of node1, use the following command:

```
awplus# atmf backup guests now node1 port1.0.23
```

**Related commands** [show atmf backup guest](#)

# atmf backup guests synchronize

**Overview** This command initiates a manual synchronization of all guest backup file-sets across remote file servers and various redundancy backup media, such as USB storage devices. This facility ensures that each device contains the same backup image files. Note that this backup synchronization process will occur as part of the regular backups scheduled by the [atmf backup](#) command.

**Syntax** `atmf backup guests synchronize`

**Default** n/a

**Mode** User Exec/Privileged Exec

**Example** To synchronize backups across remote file servers and storage devices, use the command:

```
Node1#atmf backup guests synchronize
```

**Related commands** [atmf backup redundancy enable](#)  
[show atmf guests](#)  
[atmf backup guests enable](#)

# atmf backup now

**Overview** This command initiates an immediate AMF backup of either all AMF members, or a selected AMF member. Note that this backup information is stored in the external media on the master node of the device on which this command is run, even though the selected AMF member may not be a master node.

Note that this command can only be run on an AMF master node.

**Syntax** `atmf backup now [<nodename>]`

| Parameter                      | Description   |
|--------------------------------|---|
| <nodename><br>or<br><hostname> | The name of the AMF member to be backed up, as set by the command <code>hostname</code> on page 184. Where no name has been assigned to this device, then you must use the default name, which is the word "host", then an underscore, then (without a space) the MAC address of the device to be backed up. For example <code>host_0016_76b1_7a5e</code> . Note that the node-name appears as the command Prompt when in Privileged Exec mode. |

**Default** A backup is initiated for all nodes on the AMF (but stored on the master nodes).

**Mode** Privileged Exec

**Usage notes** Although this command will select the AMF node to be backed-up, it can only be run from any AMF master node.

**NOTE:** *The backup produced will be for the selected node but the backed-up config will reside on the external media of the AMF master node on which the command was run. However, this process will result in the information on one master being more up-to-date. To maintain concurrent backups on both masters, you can apply the backup now command to the master working-set. This is shown in Example 4 below.*

**Example 1** In this example, an AMF member has not been assigned a host name. The following command is run on the `AMF_Master_2` node to immediately backup the device that is identified by its MAC address of `0016.76b1.7a5e`:

```
AMF_Master_2# atmf backup now host_0016_76b1_7a5e
```

**NOTE:** *When a host name is derived from its MAC address, the syntax format entered changes from `XXXX.XXXX.XXXX` to `XXXX_XXXX_XXXX`.*

**Example 2** In this example, an AMF member has the host name, **office\_annex**. The following command will immediately backup this device:

```
AMF_Master_2# atmf backup now office_annex
```

This command is initiated on the device's master node named **AMF\_Master\_2** and initiates an immediate backup on the device named **office\_annex**.

**Example 3** To initiate from AMF\_master\_1 an immediate backup of all AMF member nodes, use the following command:

```
AMF_Master_1# amf backup now
```

**Example 4** To initiate an immediate backup of the node with the host-name “office\_annex” and store the configuration on both masters, use the following process:

From the AMF\_master\_1, set the working-set to comprise only of the automatic group, master nodes.

```
AMF_Master_1# atmf working-set group master
```

This command returns the following display:

```
=====
AMF_Master_1, AMF_Master_2
=====

Working set join
```

Backup the AMF member with the host name, **office\_annex** on both the master nodes as defined by the working set.

```
AMF_Master[2]# atmf backup now office_annex
```

Note that the [2] shown in the command prompt indicates a 2 node working-set.

- Related commands**
- [atmf backup](#)
  - [atmf backup stop](#)
  - [hostname](#)
  - [show atmf backup](#)

# atmf backup redundancy enable

**Overview** This command is used to enable or disable AMF backup redundancy.

**Syntax** `atmf backup redundancy enable`  
`no atmf backup redundancy enable`

**Default** Disabled

**Mode** Global Configuration

**Usage notes** If the AMF Master or Controller supports any removable media (SD card/USB), it uses the removable media as the redundant backup for the AMF data backup.

This feature is valid only if remote file servers are configured on the AMF Master or Controller.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

**Example** To enable AMF backup redundancy, use the commands:

```
awplus# configure terminal
awplus(config)# atmf backup redundancy enable
```

To disable AMF backup redundancy, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf backup redundancy enable
```

**Related commands** [atmf backup synchronize](#)  
[show atmf backup](#)  
[show atmf backup area](#)

# atmf backup server

**Overview** This command configures remote file servers as the destination for AMF backups.

Use the **no** variant of this command to remove the destination server(s). When all servers are removed the system will revert to backup from external media.

**Syntax** `atmf backup server id {1|2} <hostlocation> username <username> [path <path>|port <1-65535>]`  
`no atmf backup server id {1|2}`

| Parameter      | Description  |
|----------------|--|
| id             | Remote server backup server identifier.  |
| {1 2}          | The backup server identifier number (1 or 2). Note that there can be up to two backup servers, numbered 1 and 2 respectively, and you would need to run this command separately for each server. |
| <hostlocation> | Either the name or the IP address (IPv4 or IPv6) of the selected backup server (1 or 2).   |
| username       | Configure the username to log in with on the selected remote file server.  |
| <username>     | The selected remote file server's username.  |
| path           | The location of the backup files on the selected remote file server. By default this will be the home directory of the username used to log in with.   |
| <path>         | The directory path utilized to store the backup files on the selected remote file server. No spaces are allowed in the path.   |
| port           | The connection to the selected remote backup file server using SSH. By default SSH connects to a device on TCP port 22 but this can be changed with this command.                                |
| <1-65535>      | A TCP port within the specified range.   |

**Defaults** Remote backup servers are not configured. The default SSH TCP port is 22. The path utilized on the remote file server is the home directory of the username.

**Mode** Global Exec

**Usage notes** The hostname and username parameters must both be configured.

**Examples** To configure server 1 with an IPv4 address and a username of *backup1*, use the commands:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 192.168.1.1
username backup1
```

To configure server 1 with an IPv6 address and a username of *backup1*, use the command:

```
AMF_backup1_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 FFEE::01 username
backup1
```

To configure server 2 with a hostname and username, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com
username backup2
```

To configure server 2 with a hostname and username in addition to the optional path and port parameters, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com
username backup2 path tokyo port 1024
```

To unconfigure the AMF remote backup file server 1, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# no atmf backup server id 1
```

**Related commands** [show atmf backup](#)

# atmf backup stop

**Overview** Running this command stops a backup that is currently running on the master node you are logged onto. Note that if you have two masters and want to stop both, then you can either run this command separately on each master node, or add both masters to a working set, and issue this command to the working set.

Note that this command can only be run on a master node.

**Syntax** `atmf backup stop`

**Mode** Privileged Exec

**Usage notes** This command is used to halt an AMF backup that is in progress. In this situation the backup process will finish on its current node and then stop.

**Example** To stop a backup that is currently executing on master node node-1, use the following command:

```
AMF_Master_1# amf backup stop
```

**Related commands**

- [atmf backup](#)
- [atmf backup enable](#)
- [atmf backup now](#)
- [show atmf backup](#)



# atmf backup synchronize

**Overview** For the master node you are connected to, this command initiates a system backup of files from the node's active remote file server to its backup remote file server. Note that this process happens automatically each time the network is backed up.

Note that this command can only be run from a master node.

**Syntax** `atmf backup synchronize`

**Mode** Privileged Exec

**Example** When connected to the master node `AMF_Master_1`, the following command will initiate a backup of all system related files from its active remote file server to its backup remote file server.

```
AMF_Master_1# atmf backup synchronize
```

**Related commands**

- [atmf backup enable](#)
- [atmf backup redundancy enable](#)
- [show atmf](#)
- [show atmf backup](#)

# atmf cleanup

**Overview** This command erases all data from NVS and all data from Flash **excluding** the following:

- the boot release file (a .rel file) and its release setting file
- all license files
- the latest GUI release file

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 notes** 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, a GUI resource file, and any license files, and  
then reboot the switch. Continue? (y/n):y
```

**Related commands** [erase factory-default](#)

# atmf container

**Overview** Use this command to create or update an AMF container on a Virtual AMF Appliance (VAA) virtual machine.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove an AMF container.

**Syntax** `atmf container <container-name>`  
`no atmf container <container-name>`

| Parameter                           | Description   |
|-------------------------------------|---|
| <code>&lt;container-name&gt;</code> | The name of the AMF container to create, update, or remove. |

**Mode** AMF Container Configuration

**Usage notes** You cannot delete a container while it is still running. First use the **state disable** command to stop the container.

**Examples** To create or update the AMF container "vac-wlg-1", use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)#
```

To remove the AMF container "vac-wlg-1", use the commands:

```
awplus# configure terminal
awplus(config)# no atmf container vac-wlg-1
```

**Related commands**

- [area-link](#)
- [atmf container login](#)
- [bridge-group](#)
- [description \(amf-container\)](#)
- [show atmf container](#)
- [state](#)

**Command changes** Version 5.4.7-0.1: command added

# atmf container login

**Overview** Use this command to login to an AMF container on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

**Syntax** `atmf container login <container-name>`

| Parameter                           | Description   |
|-------------------------------------|---|
| <code>&lt;container-name&gt;</code> | The name of the AMF container you wish to login into. |

**Mode** Privileged Exec

**Usage notes** If you try to login to a AMF container that has not been created, or is not running, you will see the following message:

```
% Container does not exist or is not running.
```

To exit from a container and return to the host VAA press `<Ctrl+a q>`.

**Example** To login to container “vac-wlg-1”, use the command:

```
awplus# atmf container login vac-wlg-1
```

You will then be presented with a login screen for that container:

```
Connected to tty 1
Type <Ctrl+a q> to exit the console, <Ctrl+a Ctrl+a> to enter Ctrl+a itself

vac-wlg-1 login: manager
Password: friend

AlliedWare Plus (TM) 5.4.7 02/03/17 08:46:12

vac-wlg-1>
```

**Related commands** [atmf container](#)  
[show atmf container](#)

**Command changes** Version 5.4.7-0.1: command added

# atmf controller

**Overview** Use this command to configure the device as an AMF controller. This enables you to split a large AMF network into multiple areas.

AMF controller is a licensed feature. The number of areas supported on a controller depends on the license installed on that controller.

Use the **no** variant of this command to remove the AMF controller functionality.

**Syntax** `atmf controller`  
`no atmf controller`

**Mode** Global configuration

**Usage notes** If a valid AMF controller license is not available on the device, the device will accept this command but will not act as a controller until you install a valid license. The following message will warn you of this:

“An AMF Controller license must be installed before this feature will become active”

**NOTE:** *If the AMF controller functionality is removed from a device using the **no atmf controller** command then the device must be rebooted if it is to function properly as an AMF master.*

**Example** To configure the node named *controller-1* as an AMF controller, use the commands:

```
controller-1# configure terminal
controller-1(config)# atmf controller
```

To stop the node named *controller-1* from being an AMF controller, use the commands:

```
controller-1# configure terminal
controller-1(config)# no atmf controller
```

**Related commands** `atmf area`  
`show atmf`

# atmf distribute firmware

**Overview** This command can be used to upgrade software one AMF node at a time. A URL can be selected from any media location. The latest compatible release for a node will be selected from this location.

Several procedures are performed to ensure the upgrade will succeed. This includes checking the current node release boots from flash. If there is enough space on flash the software release is copied to flash on the new location.

The new release name is updated using the `boot system` command. The old release will become the backup release file. If a release file exists in a remote device (such as TFTP or HTTP, for example) then the URL should specify the exact release filename without using a wild card character.

The command will continue to upgrade software until all nodes are upgraded. At the end of the upgrade cycle the command should be used on the working-set.

**Syntax** `atmf distribute firmware <filename>`

| Parameter                     | Description   |
|-------------------------------|---|
| <code>&lt;filename&gt;</code> | The filename and path of the file. See the <a href="#">File Management Feature Overview and Configuration Guide</a> for valid syntax. |

**Mode** Privileged Exec

**Examples** To upgrade nodes in a AMF network with a predefined AMF group called “teams”, use the following commands:

```
Team1# atmf working-set group teams
```

```
=====
Team1, Team2, Team3:
=====
Working set join
```

```
ATMF_NETWORK[3]# atmf distribute firmware card:*.rel
```

```
Retrieving data from Team1
Retrieving data from Team2
Retrieving data from Team3

ATMF Firmware Upgrade:

Node Name          New Release File          Status
-----
Team1              x510-5.4.7-1.1.rel       Release ready
Team2              x930-5.4.7-1.1.rel       Release ready
Team3              x930-5.4.7-1.1.rel       Release ready
Continue the rolling reboot ? (y/n):y
=====
Copying Release    : x510-5.4.7-1.1.rel to Team1
Updating Release   : x510-5.4.7-1.1.rel information on Team1
=====
Copying Release    : x930-5.4.7-1.1.rel to Team2
Updating Release   : x930-5.4.7-1.1.rel information on Team2
=====
Copying Release    : x930-5.4.7-1.1.rel to Team3
Updating Release   : x930-5.4.7-1.1.rel information on Team3
=====
New firmware will not take effect until nodes are rebooted.
=====

ATMF_NETWORK[3]#
```

**Related commands** [atmf working-set](#)

# atmf domain vlan

**Overview** The AMF domain VLAN is created when the AMF network is first initiated and is assigned a default VID of 4091. This command enables you to change the VID from this default value on this device.

The AMF domain VLAN is one of AMF's internal VLANs (the management VLAN is the other internal VLAN). AMF uses these internal VLANs to communicate network status information between nodes. These VLANs must be reserved for AMF and not used for other purposes.

An important point conceptually is that although the domain VLAN exists globally across the AMF network, it is assigned separately to each domain. The AMF network therefore can be thought of as comprising a series of domain VLANs each having the same VID and each being applied to a horizontal slice (domain) of the AMF. It follows therefore that the domain VLANs are only applied to ports that form cross-links and not to ports that form uplinks/downlinks.

**CAUTION:** Every member of your AMF network must have the same domain VLAN, management VLAN, and management subnet.

**CAUTION:** If you change the domain VLAN, management VLAN, or management subnet of a node, that change takes effect immediately and the node will immediately leave the AMF network and try to rejoin it. The AMF network will not be complete until you have given all devices the same setting, so they can all rejoin the AMF network.

Use the **no** variant of this command to reset the VLAN ID to its default value of 4091.

**Syntax** `atmf domain vlan <2-4090>`  
`no atmf domain vlan`

| Parameter | Description                             |
|-----------|---|
| <2-4090>  | The VLAN number in the range 2 to 4090. |

**Default** VLAN 4091

**Mode** Global Configuration

**Usage notes** We recommend you only change the domain VLAN when first creating the AMF network, and only if VLAN 4091 is already being used in your network.



However, if you do need to change the VLAN on an existing AMF network, use the following steps:

- 1) Create a working set of the whole of your AMF network, using the commands:

```
master# atmf working-set group all
```

You must use **working-set group all** if changing the domain VLAN. If you use a different working-set, nodes that are not in that working-set will lose contact with the AMF network.

- 2) The prompt will display the number of nodes in the AMF network. Record this number. In this example, the network is named "test" and has 10 nodes:

```
test[10]#
```

- 3) Enter the new VLAN ID, using the commands:

```
test[10]# configure terminal
```

```
test(config)[10]# atmf domain vlan <2-4090>
```

The nodes will execute the command in parallel, leave the AMF network, and attempt to rejoin through the new VLAN.

- 4) Create the working set again, using the commands:

```
master(config)# exit
```

```
master# atmf working-set group all
```

- 5) Save the configuration, using the command:

```
test[10]# write
```

- 6) The prompt will display the number of nodes in the AMF network. Check that this is the same as the number in step 1. If it is not, you will need to change the VLAN on missing devices by logging into their consoles directly.

**NOTE:** *The domain VLAN will automatically be assigned an IP subnet address based on the value configured by the command [atmf management subnet](#).*

The default VLAN ID lies outside the user-configurable range. If you need to reset the VLAN to the default VLAN ID, use the **no** variant of this command to do so.

**Examples** To change the AMF domain VLAN to 4090 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
```

```
test[10]# configure terminal
```

```
test(config)[10]# atmf domain vlan 4090
```

```
master(config)# exit
```

```
master# atmf working-set group all
```

```
test[10]# write
```

To reset the AMF domain VLAN to its default of 4091 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# no atmf domain vlan
master(config)# exit
master# atmf working-set group all
test[10]# write
```

**Related commands** [atmf management subnet](#)  
[atmf management vlan](#)

# atmf enable

**Overview** This command manually enables (turns on) the AMF feature for the device being configured.

Use the **no** variant of this command to disable (turn off) the AMF feature on the member node.

**Syntax** atmf enable  
no atmf enable

**Default** Once AMF is configured, the AMF feature starts automatically when the device starts up.

**Mode** Global Configuration

**Usage notes** The device does not auto negotiate AMF domain specific settings such as the Network Name. You should therefore, configure your device with any domain specific (non default) settings before enabling AMF.

**Examples** To turn off AMF, use the command:

```
MyNode# config terminal
MyNode(config)# no atmf enable
```

To turn on AMF, use the command:

```
MyNode(config)# atmf enable
```

This command returns the following display:

```
% Warning: The ATMF network config has been set to enable
% Save the config and restart the system for this change to take
effect.
```

# atmf group (membership)

**Overview** This command configures a device to be a member of one or more AMF groups. Groups exist in three forms: Implicit Groups, Automatic Groups, and User-defined Groups.

- Implicit Groups
  - all: All nodes in the AMF
  - current: The current working-set
  - local: The originating node.

Note that the Implicit Groups do not appear in show group output.

- Automatic Groups - These are defined by hardware architecture, e.g. x510, x230, x8100, AR3050S, AR4050S.
- User-defined Groups - These enable you to define arbitrary groups of AMF members based on your own criteria.

Each node in the AMF is automatically assigned membership to the implicit groups, and the automatic groups that are appropriate to its node type, e.g. x230, PoE. Similarly, nodes that are configured as masters are automatically assigned to the master group.

Use the **no** variant of this command to remove the membership.

**Syntax** `atmf group <group-list>`  
`no atmf group <group-list>`

| Parameter                       | Description  |
|---------------------------------|--|
| <code>&lt;group-list&gt;</code> | A list of group names. These should be entered as a comma delimited list without spaces. Names can contain alphanumeric characters, hyphens and underscores. |

**Mode** Global Configuration

**Usage notes** You can use this command to define your own arbitrary groups of AMF members based on your own network's configuration requirements. Applying a node to a non existing group will result in the group automatically being created.

Note that the master nodes are automatically assigned to be members of the pre-existing master group.

The following example configures the device to be members of three groups; two are company departments, and one comprises all devices located in building\_2. To avoid having to run this command separately on each device that is to be added to these groups, you can remotely assign all of these devices to a working-set, then use the capabilities of the working-set to apply the `atmf group (membership)` command to all members of the working set.

**Example 1** To specify the device to become a member of AMF groups named *marketing*, *sales*, and *building\_2*, use the following commands:

```
node-1# configure terminal
node-1(config)# atmf group marketing,sales,building_2
```

**Example 2** To add the nodes *member\_node\_1* and *member\_node\_2* to groups *building1* and *sales*, first add the nodes to the working-set:

```
master_node# atmf working-set member_node_1,member_node_2
```

This command returns the following output confirming that the nodes *member\_node\_1* and *member\_node\_2* are now part of the working-set:

```
=====
member_node_1, member_node_2
=====

Working set join
```

Then add the members of the working set to the groups:

```
atmf-net[2]# configure terminal
atmf-net[2](config)# atmf group building1,sales
atmf-net[2](config)# exit
atmf-net[2]# show atmf group
```

This command returns the following output displaying the groups that are members of the working-set.

```
=====
member_node_1
=====

AMF group information

building1, sales
```

**Related commands** [show atmf group](#)  
[show atmf group members](#)

# atmf guest-class

**Overview** This modal command creates a guest-class. Guest-classes are modal templates that can be applied to selected guest types. Once you have created a guest-class, you can select it by entering its mode. From here, you can then configure a further set of operational settings specifically for the new guest-class. These settings can then all be applied to a guest link by running the [switchport atmf-guestlink](#) command. The following settings can be configured from each guest class mode:

- discovery method
- model type
- http-enable setting
- guest port, user name, and password

The **no** variant of this command removes the guest-class. Note that you cannot remove a guest-class that is assigned to a port.

**Syntax** `atmf guest-class <guest-class-name>`  
`no atmf guest-class`

| Parameter                             | Description  |
|---------------------------------------|--|
| <code>&lt;guest-class-name&gt;</code> | The name assigned to the guest-class type. This can be chosen from an arbitrary string of up to 15 characters. |

**Mode** Interface

**Example 1** To create a guest-class named **camera** use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class camera
node1(config-atmf-guest)# end
```

**Example 2** To remove the guest-class named **phone** use the following commands:

```
node1# configure terminal
node1(config)# no atmf guest-class phone
node1(config-atmf-guest)# end
```

**Related commands**

- [show atmf area guests](#)
- [discovery](#)
- [http-enable](#)
- [username](#)
- [modeltype](#)
- [switchport atmf-guestlink](#)

show atmf links guest

show atmf guests

# atmf log-verbose

**Overview** This command limits the number of log messages displayed on the console or permanently logged.

Use the **no** variant of this command to reset to the default.

**Syntax** atmf log-verbose <1-3>  
no atmf log-verbose

| Parameter | Description   |
|-----------|---|
| <1-3>     | The verbose limitation (3 = noisiest, 1 = quietest) |

**Default** The default log display is 3.

**Usage** This command is intended for use in large networks where verbose output can make the console unusable for periods of time while nodes are joining and leaving.

**Mode** Global Configuration

**Example** To set the log-verbose to noise level 2, use the command:

```
node-1# configure terminal
node-1(config)# atmf log-verbose 2
```

**Validation Command** `show atmf`



# atmf management subnet

**Overview** This command is used to assign a subnet that will be allocated to the AMF management and domain management VLANs. From the address space defined by this command, two subnets are created, a management subnet component and a domain component, as explained in the Usage section below.

AMF uses these internal IPv4 subnets to communicate network status information between nodes. These subnet addresses must be reserved for AMF and not used for other purposes.

**CAUTION:** Every member of your AMF network must have the same domain VLAN, management VLAN, and management subnet.

**CAUTION:** If you change the domain VLAN, management VLAN, or management subnet of a node, that change takes effect immediately and the node will immediately leave the AMF network and try to rejoin it. The AMF network will not be complete until you have given all devices the same setting, so they can all rejoin the AMF network.

Use the **no** variant of this command to remove the assigned subnet.

**Syntax** atmf management subnet <a.b.0.0>  
no atmf management subnet

| Parameter | Description  |
|-----------|--|
| <a.b.0.0> | The IP address selected for the management subnet. Because a mask of 255.255.0.0 (i.e. /16) will be applied automatically, an IP address in the format a.b.0.0 must be selected. Usually this subnet address is selected from an appropriate range from within the private address space of 172.16.0.0 to 172.31.255.255, or 192.168.0.0, as defined in RFC1918. |

**Default** 172.31.0.0. A subnet mask of 255.255.0.0 will automatically be applied.

**Mode** Global Configuration

**Usage notes** Running this command will result in the creation of a further two subnets (within the class B address space assigned) and the mask will extend from /16 to /17.

For example, if the management subnet is assigned the address 172.31.0.0/16, this will result in the automatic creation of the following two subnets:

- 172.31.0.0/17 assigned to the [atmf management vlan](#)
- 172.31.128.0/17 assigned to the [atmf domain vlan](#).

We recommend you only change the management subnet when first creating the AMF network, and only if 172.31.0.0 is already being used in your network.

However, if you do need to change the subnet on an existing AMF network, use the following steps:

- 1) Create a working set of the whole of your AMF network, using the commands:

```
master# atmf working-set group all
```

You must use **working-set group all** if changing the domain VLAN, management VLAN, or management subnet. If you use a different working-set, nodes that are not in that working-set will lose contact with the AMF network.

- 2) The prompt will display the number of nodes in the AMF network. Record this number. In this example, the network is named "test" and has 10 nodes:

```
test[10]#
```

- 3) Enter the new subnet address, using the commands:

```
test[10]# configure terminal
```

```
test(config)[10]# atmf management subnet <a.b.0.0>
```

The nodes will execute the command in parallel, leave the AMF network, and attempt to rejoin through the new subnet.

- 4) Create the working set again, using the commands:

```
master(config)# exit
```

```
master# atmf working-set group all
```

- 5) Save the configuration, using the command:

```
test[10]# write
```

- 6) The prompt will display the number of nodes in the AMF network. Check that this is the same as the number in step 1. If it is not, you will need to change the subnet on missing devices by logging into their consoles directly.

**Examples** To change the AMF management subnet address to 172.25.0.0 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
```

```
test[10]# configure terminal
```

```
test(config)[10]# atmf management subnet 172.25.0.0
```

```
master(config)# exit
```

```
master# atmf working-set group all
```

```
test[10]# write
```

To reset the AMF management subnet address to its default of 172.31.0.0 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# no atmf management subnet
master(config)# exit
master# atmf working-set group all
test[10]# write
```

**Related commands**

- [atmf domain vlan](#)
- [atmf management vlan](#)

# atmf management vlan

**Overview** The AMF management VLAN is created when the AMF network is first initiated and is assigned a default VID of 4092. This command enables you to change the VID from this default value on this device.

The AMF management VLAN is one of AMF's internal VLANs (the domain VLAN is the other internal VLAN). AMF uses these internal VLANs to communicate network status information between nodes. These VLANs must be reserved for AMF and not used for other purposes.

**CAUTION:** Every member of your AMF network must have the same domain VLAN, management VLAN, and management subnet.

**CAUTION:** If you change the domain VLAN, management VLAN, or management subnet of a node, that change takes effect immediately and the node will immediately leave the AMF network and try to rejoin it. The AMF network will not be complete until you have given all devices the same setting, so they can all rejoin the AMF network.

Use the **no** variant of this command to restore the VID to the default of 4092.

**Syntax** atmf management vlan <2-4090>  
no atmf management vlan

| Parameter | Description                                  |
|-----------|--|
| <2-4090>  | The VID assigned to the AMF management VLAN. |

**Default** VLAN 4092

**Mode** Global Configuration

**Usage notes** We recommend you only change the management VLAN when first creating the AMF network, and only if VLAN 4092 is already being used in your network.

However, if you do need to change the VLAN on an existing AMF network, use the following steps to ensure you change it on all nodes simultaneously:

- 1) Create a working set of the whole of your AMF network, using the commands:

```
master# atmf working-set group all
```

You must use **working-set group all** if changing the management VLAN. If you use a different working-set, nodes that are not in that working-set will lose contact with the AMF network.

- 2) The prompt will display the number of nodes in the AMF network. Record this number. In this example, the network is named "test" and has 10 nodes:

```
test[10]#
```

- 3) Enter the new VLAN ID, using the commands:

```
test[10]# configure terminal
test(config)[10]# atmf management vlan <2-4090>
```

The nodes will execute the command in parallel, leave the AMF network, and attempt to rejoin through the new VLAN.

- 4) Create the working set again, using the commands:

```
master(config)# exit
master# atmf working-set group all
```

- 5) Save the configuration, using the command:

```
test[10]# write
```

- 6) The prompt will display the number of nodes in the AMF network. Check that this is the same as the number in step 1. If it is not, you will need to change the VLAN on missing devices by logging into their consoles directly.

**NOTE:** The management VLAN will automatically be assigned an IP subnet address based on the value configured by the command [atmf management subnet](#).

The default VLAN ID lies outside the user-configurable range. If you need to reset the VLAN to the default VLAN ID, use the **no** variant of this command to do so.

**Examples** To change the AMF management VLAN to 4090 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# atmf management vlan 4090
master(config)# exit
master# atmf working-set group all
test[10]# write
```

To reset the AMF management VLAN to its default of 4092 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# no atmf management vlan
master(config)# exit
master# atmf working-set group all
test[10]# write
```

**Related commands** [atmf domain vlan](#)  
[atmf management subnet](#)

# atmf master

**Overview** This command configures the device to be an AMF master node and automatically creates an AMF master group. The master node is considered to be the core of the AMF network, and must be present for the AMF to form. The AMF master has its node depth set to 0. Note that the node depth vertical distance is determined by the number of uplinks/downlinks that exist between the node and its master.

An AMF master node must be present for an AMF network to form. Up to two AMF master nodes may exist in a network, and they **must** be connected by an AMF crosslink.

**NOTE:** Master nodes are an essential component of an AMF network. In order to run AMF, an AMF License is required for each master node.

If the crosslink between two AMF masters fails, then one of the masters will become isolated from the rest of the AMF network.

Use the **no** variant of this command to remove the device as an AMF master node. The node will retain its node depth of 0 until the network is rebooted.

**NOTE:** Node depth is the vertical distance (or level) from the master node (whose depth value is 0).

**Syntax** atmf master  
no atmf master

**Default** The device is not configured to be an AMF master node.

**Mode** Global Configuration

**Example** To specify that this node is an AMF master, use the following command:

```
node-1# configure terminal
node-1(config)# atmf master
```

**Related commands** [show atmf](#)  
[show atmf group](#)

# atmf mtu

**Overview** This command configures the AMF network Maximum Transmission Unit (MTU). The MTU value will be applied to the AMF Management VLAN, the AMF Domain VLAN and AMF Area links.

Use the **no** variant of this command to restore the default MTU.

**Syntax** `atmf mtu <1300-1442>`  
`no atmf mtu`

| Parameter   | Description   |
|-------------|---|
| <1300-1442> | The value of the maximum transmission unit for the AMF network, which sets the maximum size of all AMF packets generated from the device. |

**Default** 1300

**Mode** Global Configuration

**Usage notes** The default value of 1300 will work for all AMF networks (including those that involve virtual links over IPsec tunnels). If there are virtual links over IPsec tunnels anywhere in the AMF network, we recommend not changing this default. If there are no virtual links over IPsec tunnels, then this AMF MTU value may be increased for network efficiency.

**Example** To change the ATMF network MTU to 1442, use the command:

```
awplus(config)# atmf mtu 1442
```

**Related commands** [show atmf detail](#)

# atmf network-name

**Overview** This command applies an AMF network name to a (prospective) AMF node. In order for an AMF network to be valid, its network-name must be configured on at least two nodes, one of which must be configured as a master and have an AMF License applied. These nodes may be connected using either AMF downlinks or crosslinks.

For more information on configuring an AMF master node, see the command [atmf master](#).

Use the **no** variant of this command to remove the AMF network name.

**Syntax** `atmf network-name <name>`  
`no atmf network-name`

| Parameter                 | Description  |
|---------------------------|--|
| <code>&lt;name&gt;</code> | The AMF network name. Up to 15 printable characters can be entered for the network-name. |

**Mode** Global Configuration

**Usage notes** This is one of the essential commands when configuring AMF and must be entered on each node that is to be part of the AMF.

A switching node (master or member) may be a member of only one AMF network.

**CAUTION:** *Ensure that you enter the correct network name. Entering an incorrect name will cause the AMF network to fragment (at the next reboot).*

**Example** To set the AMF network name to `amf_net` use the command:

```
Node_1(config)# atmf network-name amf_net
```



# atmf provision (interface)

**Overview** This command configures a specified port on an AMF node to accept a provisioned node, via an AMF link, some time in the future.

Use the **no** variant of this command to remove the provisioning on the node.

**Syntax** `atmf provision <nodename>`  
`no atmf provision`

| Parameter                     | Description   |
|-------------------------------|---|
| <code>&lt;nodename&gt;</code> | The name of the provisioned node that will appear on the AMF network in the future. |

**Mode** Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

**Usage notes** The port should be configured as an AMF link or cross link and should be “down” to add or remove a provisioned node.

**Example** To provision an AMF node named node1 for port1.0.1, use the command:

```
host1(config)# interface port1.0.1
host1(config-if)# atmf provision node1
```

**Related commands**

- `atmf provision node`
- `clone (amf-provision)`
- `configure boot config (amf-provision)`
- `configure boot system (amf-provision)`
- `copy (amf-provision)`
- `create (amf-provision)`
- `delete (amf-provision)`
- `identity (amf-provision)`
- `license-cert (amf-provision)`
- `locate (amf-provision)`
- `show atmf provision nodes`
- `show atmf links`
- `switchport atmf-link`
- `switchport atmf-crosslink`

# atmf provision node

**Overview** Use this command to provision a replacement node for a specified interface. Node provisioning is effectively the process of creating a backup file-set on a master node that can be loaded onto a provisioned node some time in the future. This file-set is created just as if the provisioned node really existed and was connected to the network. Typically these comprise configuration, operating system, and license files etc.

You can optionally provision a node with multiple device-type backups. When a device is then attached to the network, AMF uses its device-type to find the correct configuration to use. For example you can create an x510 and an x530 provisioning configuration for a node called 'node1' and if either an x510 or an x530 is attached to that node the appropriate configuration will be used.

Use the **no** variant of this command to remove a provisioned node.

**Syntax** `atmf provision node <nodename> [device <device-type>]`  
`no atmf provision node <nodename> [device <device-type>]`

| Parameter     | Description   |
|---------------|---|
| <nodename>    | The name of the provisioned node that will appear on the AMF network.   |
| device        | Optionally specify a device type.   |
| <device-type> | Any valid device type e.g. AR3050s, ie200, x950. For a full list of valid device types use the command <b>atmf provision node &lt;nodename&gt; device ?</b> . |

**Mode** Privileged Exec

**Usage notes** This command creates the directory structure for the provisioned node's file-set. It also switches to the AMF provision node prompt so that the nodes backup file-set can be created or updated. This is typically done with the [create \(amf-provision\)](#) or [clone \(amf-provision\)](#) commands.

For more information on AMF provisioning, see the [AMF Feature Overview and Configuration Guide](#)..

**Example** To configure node named 'node1', use the command:

```
awplus# atmf provision node node1  
awplus(atmf-provision)#
```

To configure a node named 'node1' for device type 'x530', use the command:

```
awplus# atmf provision node node1 device x530  
awplus(atmf-provision)#
```

**Related commands**

- atmf provision (interface)
- clone (amf-provision)
- configure boot config (amf-provision)
- configure boot system (amf-provision)
- copy (amf-provision)
- create (amf-provision)
- delete (amf-provision)
- identity (amf-provision)
- license-cert (amf-provision)
- locate (amf-provision)
- show atmf provision nodes

**Command changes** Version 5.4.9-0.1: command added

# atmf reboot-rolling

**Overview** This command enables you to reboot the nodes in an AMF working-set, one at a time, as a rolling sequence in order to minimize downtime. Once a rebooted node has finished running its configuration and its ports are up, it re-joins the AMF network and the next node is rebooted.

By adding the *url* parameter, you can also upgrade your devices' software one AMF node at a time.

The **force** parameter forces the rolling reboot to continue even if a previous node does not rejoin the AMF network. Without the **force** parameter, the unsuitable node will time-out and the rolling reboot process will stop. However, with the **force** parameter applied, the process will ignore the timeout and move on to reboot the next node in the sequence.

This command can take a significant amount of time to complete.

**Syntax** `atmf reboot-rolling [force] [<url>]`

| Parameter                | Description  |
|--------------------------|--|
| <code>force</code>       | Ignore a failed node and move on to the next node. Where a node fails to reboot a timeout is applied based on the time taken during the last reboot. |
| <code>&lt;url&gt;</code> | The path to the software upgrade file.   |

**Mode** Privileged Exec

**Usage notes** You can load the software from a variety of locations. The latest compatible release for a node will be selected from your selected location, based on the parameters and URL you have entered.

For example `card:/5.4.6/x*-5.4.6-*.rel` will select from the folder `card:/5.4.6` the latest file that matches the selection `x` (wildcard) `-5.4.6-` (wildcard).`rel`. Because `x*` is applied, each device type will be detected and its appropriate release file will be installed.

Other allowable entries are:

| Entry                                 | Used when loading software                              |
|---------------------------------------|---|
| <code>card:*.rel:</code>              | from an SD card   |
| <code>tftp:&lt;ip-address&gt;:</code> | from a TFTP server                                      |
| <code>usb:</code>                     | from a USB flash drive                                  |
| <code>flash:</code>                   | from flash memory, e.g. from one x930 switch to another |
| <code>scp:</code>                     | using secure copy                                       |
| <code>http:</code>                    | from an HTTP file server                                |

Several checks are performed to ensure the upgrade will succeed. These include checking the current node release boots from flash. If there is enough space on flash, the software release is copied to flash to a new location on each node as it is processed. The new release name will be updated using the **boot system**<release-name> command, and the old release will become the backup release file.

**NOTE:** *If you are using TFTP or HTTP, for example, to access a file on a remote device then the URL should specify the exact release filename without using wild card characters.*

On bootup the software release is verified. Should an upgrade fail, the upgrading unit will revert back to its previous software version. At the completion of this command, a report is run showing the release upgrade status of each node.

**NOTE:** *Take care when removing external media or rebooting your devices. Removing an external media while files are being written entails a significant risk of causing a file corruption.*

**Example 1** To reboot all x510 nodes in an AMF network, use the following command:

```
Bld2_Floor_1# atmf working-set group x510
```

This command returns the following type of screen output:

```
=====
node1, node2, node3:
=====

Working set join

AMF_NETWORK[3]#
```

```
ATMF_NETWORK[3]# atmf reboot-rolling
```

When the reboot has completed, a number of status screens appear. The selection of these screens will depend on the parameters set.

```
Bld2_Floor_1#atmf working-set group x510

=====
SW_Team1, SW_Team2, SW_Team3:
=====

Working set join

ATMF_NETWORK[3]#atmf reboot-rolling
ATMF Rolling Reboot Nodes:

Node Name                Timeout
                        (Minutes)
-----
SW_Team1                  14
SW_Team2                   8
SW_Team3                   8
Continue the rolling reboot ? (y/n):y
=====
ATMF Rolling Reboot: Rebooting SW_Team1
=====

% SW_Team1 has left the working-set
Reboot of SW_Team1 has completed
=====
ATMF Rolling Reboot: Rebooting SW_Team2
=====

% SW_Team2 has left the working-set
Reboot of SW_Team2 has completed
=====
ATMF Rolling Reboot: Rebooting SW_Team3
=====

% SW_Team3 has left the working-set
Reboot of SW_Team3 has completed

=====
ATMF Rolling Reboot Complete
Node Name                Reboot Status
-----
SW_Team1                  Rebooted
SW_Team2                  Rebooted
SW_Team3                  Rebooted
=====
```

**Example 2** To update firmware releases, use the following command:

```
Node_1# atmf working-set group all

ATMF_NETWORK[9]# atmf reboot-rolling
card:/5.4.6/x*-5.4.6-*.rel
```

```
ATMF Rolling Reboot Nodes:
```

| Node Name    | Timeout<br>(Minutes) | New Release File   | Status        |
|--------------|----------------------|--------------------|---------------|
| SW_Team1     | 8                    | x510-5.4.6-0.1.rel | Release Ready |
| SW_Team2     | 10                   | x510-5.4.6-0.1.rel | Release Ready |
| SW_Team3     | 8                    | ---                | Not Supported |
| HW_Team1     | 6                    | ---                | Incompatible  |
| Bld1_Floor_2 | 2                    | x930-5.4.6-0.1.rel | Release Ready |
| Bld1_Floor_1 | 4                    | ---                | Incompatible  |
| Building_1   | 2                    | ---                | Incompatible  |
| Building_2   | 2                    | x908-5.4.6-0.1.rel | Release Ready |

Continue upgrading releases ? (y/n):

# atmf recover

**Overview** This command is used to manually initiate the recovery (or replication) of an AMF node, usually when a node is being replaced.

**Syntax** `atmf recover [<node-name> master <node-name>]`  
`atmf recover [<node-name> controller <node-name>]`

| Parameter                           | Description  |
|-------------------------------------|--|
| <i>&lt;node-name&gt;</i>            | The name of the device whose configuration is to be recovered or replicated.   |
| master<br><i>&lt;node-name&gt;</i>  | The name of the master device that holds the required configuration information.<br>Note that although you can omit both the node name and the master name; you cannot specify a master name unless you also specify the node name.      |
| controller <i>&lt;node-name&gt;</i> | The name of the controller that holds the required configuration information.<br>Note that although you can omit both the node name and the controller name; you cannot specify a controller name unless you also specify the node name. |

**Mode** Privileged Exec

**Usage notes** The recovery/replication process involves loading the configuration file for a node that is either about to be replaced or has experienced some problem. You can specify the configuration file of the device being replaced by using the *<node-name>* parameter, and you can specify the name of the master node or controller holding the configuration file.

If the *<node-name>* parameter is not entered then the node will attempt to use one that has been previously configured. If the replacement node has no previous configuration (and has no previously used node-name), then the recovery will fail.

If the master or controller name is not specified then the device will poll all known AMF masters and controllers and execute an election process (based on the last successful backup and its timestamp) to determine which to use. If no valid backup master or controller is found, then this command will fail.

No error checking occurs when this command is run. Regardless of the last backup status, the recovering node will attempt to load its configuration from the specified master node or controller.

If the node has previously been configured, we recommend that you suspend any AMF backup before running this command. This is to prevent corruption of the backup files on the AMF master as it attempts to both backup and recover the node at the same time.



**Example** To recover the AMF node named Node\_10 from the AMF master node named Master\_2, use the following command:

```
Master_2# atmf recover Node_10 master Master_2
```

**Related commands**

- atmf backup stop
- show atmf backup
- show atmf

# atmf recover guest

**Overview** Use this command to initiate a guest node recovery or replacement by reloading its backup file-set that is located within the AMF backup system. Note that this command must be run on the edge node device that connects to the guest node.

**Syntax** `atmf recover guest [<guest-port>]`

| Parameter                       | Description                                      |
|---------------------------------|--|
| <code>&lt;guest-port&gt;</code> | The port number that connects to the guest node. |

**Mode** User Exec/Privileged Exec

**Example** To recover a guest on node1 port1.0.1, use the following command

```
node1# atmf recover guest port1.0.1
```

**Related commands** [show atmf backup guest](#)

# atmf recover led-off

**Overview** This command turns off the recovery failure flashing port LEDs. It reverts the LED's function to their normal operational mode, and in doing so assists with resolving the recovery problem. You can repeat this process until the recovery failure has been resolved. For more information, see the [AMF Feature Overview and Configuration Guide](#).

**Syntax** `atmf recover led-off`

**Default** Normal operational mode

**Mode** Privileged Exec

**Example** To revert the LEDs on Node1 from recovery mode display to their normal operational mode, use the command:

```
Node1# atmf recover led-off
```

**Related commands** [atmf recover](#)

# atmf recovery-server

**Overview** Use this command on an AMF master to process recovery requests from isolated AMF nodes. An isolated node is an AMF member that is only connected to the rest of the AMF network via a virtual-link.

This option allows these nodes, which have no AMF neighbors, to be identified for recovery or provisioning purposes. They are identified using an identity token which is stored on the AMF master.

Use the **no** variant of this command to disable processing of recovery requests from isolated AMF nodes.

**Syntax** `atmf recovery-server`  
`no atmf recovery-server`

**Default** Recovery-server is disabled by default.

**Mode** Global Configuration

**Usage notes** Once **recovery-server** is enabled on an AMF network, the next time an isolated node is backed up its identity token will be stored in the AMF master's database. Should the device fail it can then be replaced and auto-recovery will occur as long as:

- the AMF master is accessible to the isolated node, and
- either, a DHCP server is configured to send the Uniform Resource Identifier (URI) of the AMF master to the recovering node, or
- a DNS server is configured to resolve the default recovery URI (`https://amfrecovery.alliedtelesis.com`) to the IP address of the AMF master.

Provisioning of isolated nodes is achieved by creating an identity token for the new node using the [identity \(amf-provision\)](#) command.

See the [AMF Feature Overview and Configuration Guide](#) for information on preparing your network for recovering or provisioning isolated nodes.

**Example** To enable recovery-server on an AMF master, use the commands:

```
awplus# configure terminal
awplus(config)# atmf recovery-server
```

To disable recovery-server on an AMF master, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf recovery-server
```

**Related commands**

- [atmf backup](#)
- [atmf cleanup](#)
- [identity \(amf-provision\)](#)
- [atmf virtual-link](#)

**Command changes** Version 5.4.7-2.1: command added

# atmf remote-login

**Overview** Use this command to remotely login to other AMF nodes in order to run commands as if you were a local user of that node.

**Syntax** `atmf remote-login [user <name>] <nodename>`

| Parameter  | Description  |
|------------|--|
| <name>     | The name of a user on the remote node.                 |
| <nodename> | The name of the remote AMF node you are connecting to. |

**Mode** Privileged Exec (This command will only run at privilege level 15)

**Usage notes** You do not need a valid login on the local device in order to run this command. The session will take you to the enable prompt on the new device. If the remote login session exits for any reason (e.g. device reboot) you will be returned to the originating node.

You can create additional user accounts on nodes. AMF's goal is to provide a uniform management plane across the whole network, so we recommend you use the same user accounts on all the nodes in the network.

In reality, though, it is not essential to have the same accounts on all the nodes. Users can remote login from one node to a second node even if they are logged into the first node with a user account that does not exist on the second node (provided that `atmf restricted-login` is disabled and the user account on the first node has privilege level 15).

Moreover, it is possible to use a RADIUS or TACACS+ server to manage user authentication, so users can log into AMF nodes using user accounts that are present on the RADIUS or TACACS+ server, and not present in the local user databases of the AMF nodes.

The software will not allow you to run multiple remote login sessions. You must exit an existing session before starting a new one.

If you disconnect from the VTY session without first exiting from the AMF remote session, the device will keep the AMF remote session open until the `exec-timeout` time expires (10 minutes by default). If the `exec-timeout` time is set to infinity (`exec-timeout 0 0`), then the device is unable to ever close the remote session. To avoid this, we recommend you use the `exit` command to close AMF remote sessions, instead of closing the associated VTY sessions. We also recommend you avoid setting the `exec-timeout` to infinity.

**Example** To remotely login from node Node10 to Node20, use the following command:

```
Node10# atmf remote-login node20
Node20>
```

To close the session on Node20 and return to Node10's command line, use the following command:

```
Node20# exit  
Node10#
```

In this example, user User1 is a valid user of node5. They can remotely login from node5 to node3 by using the following commands:

```
node5# atmf remote-login user User1 node3  
node3> enable
```

**Related commands** [atmf restricted-login](#)

**Command changes** Version 5.4.6-2.1: changes to AMF user account requirements

# atmf restricted-login

**Overview** By default, users who are logged into any node on an AMF network are able to manage any other node by using either working-sets or an AMF remote login. If the access provided by this feature is too wide, or contravenes network security restrictions, it can be limited by running this command, which changes the access so that:

- users who are logged into non-master nodes cannot execute any commands that involve working-sets, and
- from non-master nodes, users can use remote-login, but only to login to a user account that is valid on the remote device (via a statically configured account or RADIUS/TACACS+). Users are also required to enter the password for that user account.

Once entered on any AMF master node, this command will propagate across the network.

Use the **no** variant of this command to disable restricted login on the AMF network. This allows access to the **atmf working-set** command from any node in the AMF network.

**Syntax** `atmf restricted-login`  
`no atmf restricted-login`

**Mode** Privileged Exec

**Default** Master nodes operate with **atmf restricted-login** disabled.  
Member nodes operate with **atmf restricted-login** enabled.

**NOTE:** *The default conditions of this command vary from those applied by its “no” variant. This is because the restricted-login action is only applied by **master** nodes, and in the absence of a master node, the default is to apply the restricted action to all **member** nodes with AMF configured.*

**Usage notes** In the presence of a **master** node, its default of **atmf restricted-login disabled** will propagate to all its member nodes. Similarly, any change in this command’s status that is made on a master node, will also propagate to all its member nodes

Note that once you have run this command, certain other commands that utilize the AMF working-set command, such as the **include**, **atmf reboot-rolling** and **show atmf group members** commands, will operate only on master nodes.

Restricted-login must be enabled on AMF areas with more than 120 nodes.

**Example** To enable restricted login, use the command

```
Node_20(config)# atmf restricted-login node20
```

**Related commands** `atmf remote-login`  
`show atmf`



**Command changes** Version 5.4.6-2.1: changes to AMF user account requirements

# atmf secure-mode

**Overview** Use this command to enable AMF secure mode on an AMF node. AMF secure mode makes an AMF network more secure by:

- Adding an authorization mechanism before and AMF member is allowed to join an AMF network.
- The encryption of all AMF packets sent between AMF nodes.
- Adding support for user login authentication by RADIUS or TACACS+, and removing the requirement to have the same privileged user account in the local user database on all devices in the AMF network.
- Adding additional logging which enables network administrators to monitor attempts to gain unauthorized access to the AMF network.

Once the secure mode command is run on all nodes on an AMF network, the AMF masters and AMF controllers manage the addition of AMF nodes and AMF areas to the AMF network.

Use the **no** variant of this command to disable AMF secure mode on an AMF node.

**Syntax** `atmf secure-mode`  
`no atmf secure-mode`

**Default** Secure mode is disabled by default.

**Mode** Global Configuration

**Usage notes** When an AMF network is running in AMF secure mode the [atmf restricted-login](#) feature is automatically enabled. This restricts the [atmf working-set](#) command to users that are logged on to an AMF master. This feature cannot be disabled independently of secure mode.

When AMF secure mode is enabled the AMF controllers and masters in the AMF network form a group of certificate authorities. A node may only join a secure AMF network once it has been authorized by a master or controller. When enabled, all devices in the AMF network must be running in secure mode. Unsecured devices will not be able to join a secure AMF network.

**Example** To enable AMF secure mode on an AMF node, use the commands:

```
awplus# configure terminal
awplus(config)# atmf secure-mode
```

To disable AMF secure mode on an AMF node, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf secure-mode
```

**Related commands** [atmf authorize](#)  
[atmf secure-mode certificate expiry](#)

clear atmf secure-mode certificates  
clear atmf secure-mode statistics  
show atmf  
show atmf authorization  
show atmf secure-mode  
show atmf secure-mode certificates  
show atmf secure-mode sa  
show atmf secure-mode statistics

**Command changes** Version 5.4.7-0.3: command added

# atmf secure-mode certificate expire

**Overview** Use this command on an AMF master to expire a secure mode certificate. Running this command will force the removal of the AMF node from the network.

**Syntax** `atmf secure-mode certificate expire <node-name> [area <area-name>]`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;node-name&gt;</code> | Name of the AMF node you want to expire the certificate for.           |
| <code>area</code>              | Specify an AMF area.   |
| <code>&lt;area-name&gt;</code> | Name of the AMF area you want to expire the AMF nodes certificate for. |

**Mode** Privileged Exec

**Example** To remove an AMF node named "node3" from an AMF network, use the following command on the AMF master:

```
awplus# atmf secure-mode certificate expire node3
```

To remove an AMF node named "node2" in an area named "area2", use the following command on the AMF master:

```
awplus# atmf secure-mode certificate expire node2 area area2
```

**Related commands**

- [atmf secure-mode](#)
- [show atmf secure-mode](#)
- [show atmf secure-mode certificates](#)

**Command changes** Version 5.4.7-0.3: command added

# atmf secure-mode certificate expiry

**Overview** Use this command to set the expiry time of AMF secure mode certificates. Once an AMF node's certificate expires it must re-authorize and obtain a new certificate from the AMF master.

Use the **no** variant of this command to reset the expiry time to 180 days.

**Syntax** `atmf secure-mode certificate expiry {<days>|infinite}`  
`no atmf secure-mode certificate expiry`

| Parameter                 | Description  |
|---------------------------|--|
| <code>&lt;days&gt;</code> | Length of time, in days, that an AMF secure mode certificate remains valid. A value between 1 and 365. |
| <code>infinite</code>     | The authorization certificate does not expire, in other words AMF nodes stay authorized indefinitely.  |

**Default** The default expiry time is 180 days.

**Mode** Global Configuration

**Example** To set AMF secure mode certificate expiry to 7 days, use the commands:

```
awplus# configure terminal
awplus(config)# atmf secure-mode certificate expiry 7
```

To set AMF secure mode certificates to never expire, use the commands:

```
awplus# configure terminal
awplus(config)# atmf secure-mode certificate expiry infinite
```

To reset the certificate expiry to 180 days, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf secure-mode certificate expiry
```

**Related commands** [atmf secure-mode](#)  
[show atmf secure-mode](#)  
[show atmf secure-mode certificates](#)

**Command changes** Version 5.4.7-0.3: command added

# atmf secure-mode certificate renew

**Overview** Use this command to force all local certificates to expire and be renewed on an AMF secure mode network.

Secure mode certificates renew automatically but this command could be used to renew a certificate in a situation where the automatic renewal may happen while the device is not attached to the AMF network.

**Syntax** `atmf secure-mode certificate renew`

**Mode** Privileged Exec

**Example** To renew a local certificate on a AMF member or AMF master, use the command:

```
awplus# atmf secure-mode certificate renew
```

**Related commands** [show atmf secure-mode certificates](#)  
[show atmf secure-mode statistics](#)

**Command changes** Version 5.4.7-0.3: command added

# atmf secure-mode enable-all

**Overview** Use this command to enable AMF secure mode on an entire network. AMF secure mode makes an AMF network more secure by:

- Adding an authorization mechanism before an AMF member is allowed to join an AMF network.
- The encryption of all AMF packets sent between AMF nodes.
- Adding support for user login authentication by RADIUS or TACACS+, and removing the requirement to have the same privileged user account in the local user database on all devices in the AMF network.
- Adding additional logging which enables network administrators to monitor attempts to gain unauthorized access to the AMF network.

Once this command is run on an AMF network, the AMF masters and AMF controllers manage the addition of AMF nodes and AMF areas to the AMF network.

This command can only be run on an AMF master.

Use the **no** variant of this command to disable AMF secure mode on an entire network.

**Syntax** `atmf secure-mode enable-all`  
`no atmf secure-mode enable-all`

**Default** Secure mode is disabled by default.

**Mode** Privileged Exec

**Usage notes** When an AMF network is running in AMF secure mode the [atmf restricted-login](#) feature is automatically enabled. This restricts the [atmf working-set](#) command to users that are logged on to an AMF master. This feature cannot be disabled independently of secure mode.

When AMF secure mode is enabled the AMF controllers and masters in the AMF network form a group of certificate authorities. A node may only join a secure AMF network once it has been authorized by a master or controller. When enabled, all devices in the AMF network must be running in secure mode. Unsecured devices will not be able to join a secure AMF network.

Running **atmf secure-mode enable-all**:

- Groups all AMF members in a working set.
- Executes [clear atmf secure-mode certificates](#) on the working set of members, which removes existing secure mode certificates from all the nodes.
- Groups all the AMF masters in a working set.
- Executes [atmf authorize provision all](#) on the working set of masters, so all masters provision all nodes.
- Groups all AMF nodes in a working set.

- Runs a script which executes `atmf secure-mode` and then writes the configuration file on each node.
- Starts a timer that ticks every 10 seconds, for a maximum of 10 times, and checks if all the secure mode capable nodes rejoin the AMF network.

Running **no atmf secure-mode enable-all**:

- Groups all AMF nodes in a working set.
- Runs a script which executes **no atmf secure-mode** and then writes the configuration file on each node.
- Starts a timer that ticks every 10 seconds, for a maximum of 10 times, and checks if all the secure mode capable nodes rejoin the AMF network.

**NOTE:** Enabling or disabling secure mode on the network saves the running-config on every device.

**Example** To enable AMF secure mode on the entire network, use the command:

```
awplus# atmf secure-mode enable-all
```

You will be prompted to confirm the action:

```
Total number of nodes 21
21 nodes support secure-mode

Enable secure-mode across the AMF network ? (y/n): y
```

To disable AMF secure mode on the entire network, use the command:

```
awplus# no atmf secure-mode enable-all
```

You will be prompted to confirm the action:

```
% Warning: All security certificates will be deleted.
Disable secure-mode across the AMF network ? (y/n): y
```

**Related commands** `show atmf`

**Command changes** Version 5.4.7-0.3: command added



# atmf select-area

**Overview** Use this command to access devices in an area outside the core area on the controller network. This command will connect you to the remote area-master of the specified area.

This command is only valid on AMF controllers.

The **no** variant of this command disconnects you from the remote area-master.

**Syntax** `atmf select-area {<area-name>|local}`  
`no atmf select-area`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;area-name&gt;</code> | Connect to the remote area-master of the area with this name. |
| <code>local</code>             | Return to managing the local controller area.                 |

**Mode** Privileged Exec

**Usage notes** After running this command, use the [atmf working-set](#) command to select the set of nodes you want to access in the remote area.

**Example** To access nodes in the area Canterbury, use the command

```
controller-1# atmf select-area Canterbury
```

This displays the following output:

```
Test_network[3]#atmf select-area Canterbury
=====
Connected to area Canterbury via host Avensis:
=====
```

To return to the local area for controller-1, use the command

```
controller-1# atmf select-area local
```

Alternatively, to return to the local area for controller-1, use the command

```
controller-1# no atmf select-area
```

**Related commands** [atmf working-set](#)

# atmf topology-gui enable

**Overview** Use this command to enable the operation of Vista Manager EX on the Master device.

Vista Manager EX delivers state-of-the-art monitoring and management for your Autonomous Management Framework™ (AMF) network, by automatically creating a complete topology map of switches, firewalls and wireless access points (APs). An expanded view includes third-party devices such as security cameras.

Use the **no** variant of this command to disable operation of Vista Manager EX.

**Syntax** atmf topology-gui enable  
no atmf topology-gui enable

**Default** Disabled by default on AMF Master and member nodes. Enabled by default on Controllers.

**Mode** Global Configuration mode

**Usage notes** To use Vista Manager EX, you must also enable the HTTP service on all AMF nodes, including all AMF masters and controllers. The HTTP service is enabled by default on AlliedWare Plus switches and disabled by default on AR-Series firewalls. To enable it, use the commands:

```
Node1# configure terminal
Node1(config)# service http
```

On one master in each AMF area in your network, you also need to configure the master to send event notifications to Vista Manager EX. To do this, use the commands:

```
Node1# configure terminal
Node1(config)# log event-host <ip-address> atmf-topology-event
```

**Example** To enable Vista Manager EX on Node1, use the following commands:

```
Node1# configure terminal
Node1(config)# atmf topology-gui enable
```

To disable Vista Manager EX on Node1, use the following commands:

```
Node1# configure terminal
Node1(config)# no atmf topology-gui enable
```

**Related commands** [atmf enable](#)  
[log event-host](#)  
[service http](#)

# atmf trustpoint

**Overview** Use this command to set a PKI trustpoint for an AMF network. This command needs to be run on an AMF master or controller.

The self-signed certificate authority (CA) certificate is distributed to every node on the AMF network. It is used to verify client certificates signed by the trustpoint.

Use the **no** variant of this command to remove an AMF trustpoint.

**Syntax** `atmf trustpoint <trustpoint-name>`  
`no atmf trustpoint <trustpoint-name>`

| Parameter                            | Description             |
|--------------------------------------|-------------------------|
| <code>&lt;trustpoint-name&gt;</code> | Name of the trustpoint. |

**Default** No trustpoint is configured by default.

**Mode** Global Configuration

**Usage notes** Before using the **atmf trustpoint** command you will need to establish a trustpoint. For example, you can create a local self-signed trustpoint using the procedure outlined below.

Create a self-signed trustpoint called 'our\_trustpoint' with keypair 'our\_key':

```
awplus# configure terminal
awplus(config)# crypto pki trustpoint our_trustpoint
awplus(ca-trustpoint)# enrollment selfsigned
awplus(ca-trustpoint)# rsakeypair our_key
awplus(ca-trustpoint)# exit
awplus(config)# exit
```

Create the root and server certificates for this trustpoint:

```
awplus# crypto pki authenticate our_trustpoint
awplus# crypto pki enroll our_trustpoint
```

For more information about the AlliedWare Plus implementation of Public Key Infrastructure (PKI), see the [Public Key Infrastructure \(PKI\) Feature Overview and Configuration Guide](#)

**Example** To configure an AMF trustpoint for the trustpoint 'our\_trustpoint', use the commands:

```
awplus# configure terminal
awplus(config)# atmf trustpoint our_trustpoint
```

To remove an AMF trustpoint for the trustpoint 'our\_trustpoint', use the commands:

```
awplus# configure terminal
awplus(config)# no atmf trustpoint our_trustpoint
```

**Related commands** [crypto pki trustpoint](#)  
[show atmf](#)

**Command changes** Version 5.4.7-2.1: command added

# atmf virtual-crosslink

**Overview** Use this command to create a virtual crosslink. A virtual crosslink connects an AMF master or controller on a physical device to a Virtual AMF Appliance (VAA) master or controller.

All AMF master nodes must reside in the same AMF domain and are required to be directly connected using AMF crosslinks. In order to be able to meet this requirement for AMF masters running on VAAs, a virtual crosslink connects the AMF master or controller on the physical device to the master or controller on the VAA.

Use the **no** variant of this command to remove a virtual crosslink.

**Syntax** `atmf virtual-crosslink id <local-id> ip <local-ip> remote-id <remote-id> remote-ip <remote-ip>`  
`no atmf virtual-crosslink id <local-id>`

| Parameter   | Description   |
|-------------|---|
| <local-id>  | ID of the local tunnel port, a value between 1 and 4094.  |
| <local-ip>  | IPv4 address of the local tunnel port in a.b.c.d format.  |
| <remote-id> | ID of the remote tunnel port, a value between 1 and 4094. |
| <remote-ip> | IPv4 address of the remote tunnel port in a.b.c.d format. |

**Default** No AMF virtual crosslinks are created by default.

**Mode** Global Configuration

**Usage notes** This command allows a virtual tunnel to be created between two remote sites over a layer 3 link. The tunnel encapsulates AMF packets and allows them to be sent transparently across a Wide Area Network (WAN) such as the Internet.

Configuration involves creating a local tunnel ID, a local IP address, a remote tunnel ID and a remote IP address. Each side of the tunnel must be configured with the same, but mirrored parameters.

**NOTE:** *Virtual crosslinks are not supported on AMF container masters, therefore if multiple tenants on a single VAA host are configured for secure mode, only a single AMF master is supported per area.*

**Example** To setup a virtual link from a local site, "siteA", to a remote site, "siteB", (assuming there is already IP connectivity between the sites), run the following commands at the local site:

```
siteA# configure terminal
siteA(config)# atmf virtual-crosslink id 5 ip 192.168.100.1
remote-id 10 remote-ip 192.168.200.1
```

At the remote site, run the commands:

```
siteB# configure terminal
siteB(config)# atmf virtual-crosslink id 10 ip 192.168.200.1
remote-id 5 remote-ip 192.168.100.1
```

To remove this virtual crosslink, run the following commands on the local site:

```
siteA# configure terminal
siteA(config)# no atmf virtual-crosslink id 5
```

On the remote site, run the commands:

```
siteB# configure terminal
siteB(config)# no atmf virtual-crosslink id 10
```

**Related  
commands**

[atmf virtual-crosslink](#)  
[show atmf links](#)  
[switchport atmf-crosslink](#)

**Command  
changes**

Version 5.4.7-0.3: command added

# atmf virtual-link

**Overview** This command creates one or more Layer 2 tunnels that enable AMF nodes to transparently communicate across a wide area network using Layer 2 connectivity protocols.

Once connected through the tunnel, the remote member will have the same AMF capabilities as a directly connected AMF member.

Use the **no** variant of this command to remove the specified virtual link.

**Syntax**

```
atmf virtual-link id <1-4094> ip <a.b.c.d> remote-id <1-4094>  
remote-ip <a.b.c.d> [remote-area <area-name>]  
  
atmf virtual-link id <1-4094> interface <interface-name>  
remote-id <1-4094> remote-ip <a.b.c.d> [remote-area  
<area-name>]  
  
no atmf virtual-link id <1-4094>
```

| Parameter                     | Description   |
|-------------------------------|---|
| id <1-4094>                   | ID of the local tunnel point, in the range 1 to 4094.   |
| ip <a.b.c.d>                  | Specify the local IP address of the local interface for the virtual-link (alternatively you can specify the interface's name, see below).   |
| interface<br><interface-name> | Specify the local interface name for the virtual-link. This allows you to use a dynamic, rather than a static, local IP address.  |
| remote-id<1-4094>             | The ID of the (same) tunnel that will be applied by the remote node. Note that this must match the local-id that is defined on the remote node. This means that (for the same tunnel) the local and remote tunnel IDs are reversed on the local and remote nodes. |
| remote-ip<br><a.b.c.d>        | The IP address of the remote node.  |
| remote-area<br><area-name>    | The name of the remote area connected to this virtual-link  |

**Mode** Global Configuration

**Usage notes** The Layer 2 tunnel that this command creates enables a local AMF session to appear to pass transparently across a Wide Area Network (WAN) such as the Internet. The addresses configured as the local and remote tunnel IP addresses must have IP connectivity to each other. If the tunnel is configured to connect a head office and branch office over the Internet, typically this would involve using some type of managed WAN service such as a site-to-site VPN. Tunnels are only supported using IPv4.

Configuration involves creating a local tunnel ID, a local IP address, a remote tunnel ID and a remote IP address. A reciprocal configuration is also required on the corresponding remote device. The local tunnel ID must be unique to the device on which it is configured.

If an interface acquires its IP address dynamically then the local side of the tunnel can be specified by using the interface's name instead of using its IP address. When using a dynamic local address the remote address of the other side of the virtual-link must be configured with either:

- the IP address of the NAT device the dynamically configured interface is behind, or
- 0.0.0.0, if the virtual-link is configured as a secure virtual-link.

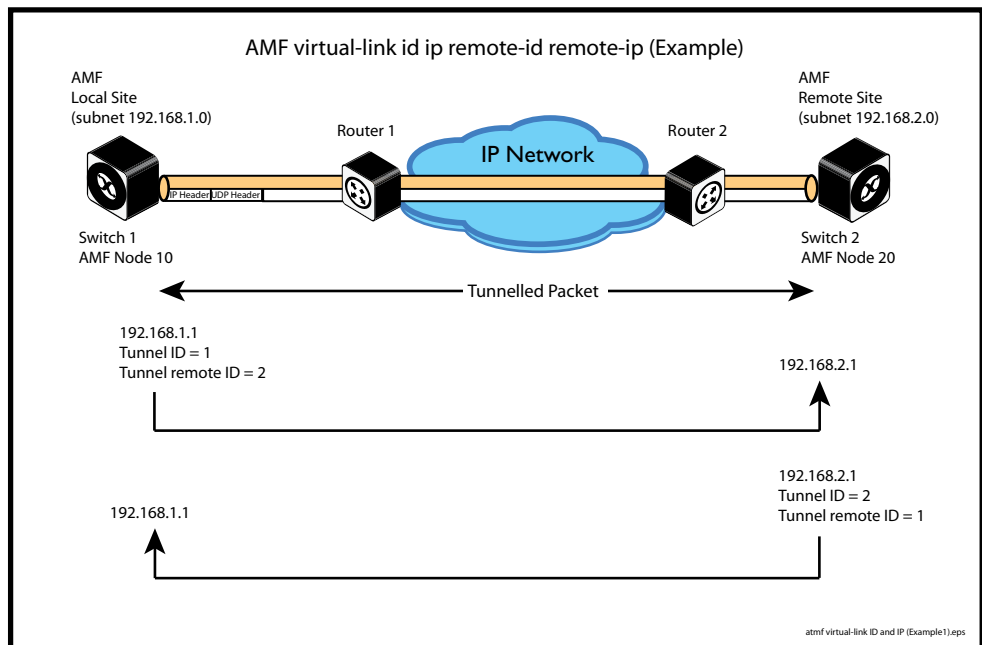
For instructions on how to configure dynamic IP addresses on virtual-links, see the [AMF Feature Overview and Configuration Guide](#).

The tunneled link may operate via external (non AlliedWare Plus) routers in order to provide wide area network connectivity. However in this configuration, the routers perform a conventional router to router connection. The protocol tunneling function is accomplished by the AMF nodes.

**NOTE:** AMF cannot achieve zero touch replacement of the remote device that terminates the tunnel connection, because you must pre-configure the local IP address and tunnel ID on that remote device.

**Example 1** Use the following commands to create the tunnel shown in the figure below.

Figure 19-1: AMF virtual link example



```
Node_10(config)# atmf virtual-link id 1 ip 192.168.1.1
remote-id 2 remote-ip 192.168.2.1

Node_20(config)# atmf virtual-link id 2 ip 192.168.2.1
remote-id 1 remote-ip 192.168.1.1
```



**Example 2** To set up an area virtual link to a remote site (assuming IP connectivity between the sites already), one site must run the following commands:

```
SiteA# configure terminal
SiteA(config)# atmf virtual-link id 5 ip 192.168.100.1
remote-id 10 remote-ip 192.168.200.1 remote-area SiteB-AREA
```

The second site must run the following commands:

```
SiteB# configure terminal
SiteB(config)# atmf virtual-link id 10 ip 192.168.200.1
remote-id 5 remote-ip 192.168.100.1 remote-area SiteA-AREA
```

Before you can apply the above **atmf virtual-link** command, you must configure the area names *SiteB-AREA* and *SiteA-AREA*.

**Related commands**

- [atmf virtual-link protection](#)
- [show atmf](#)
- [show atmf links](#)
- [show atmf virtual-links](#)

**Command changes** Version 5.4.9-0.1: **interface** parameter added

# atmf virtual-link protection

**Overview** Use this command to add protection to an existing AMF virtual-link. Secure AMF virtual-links encapsulate the L2TPv3 frames of the virtual-link with IPsec.

Use the **no** variant of this command to remove protection from an AMF virtual-link.

**Syntax**

```
atmf virtual-link id <1-4094> protection ipsec key [8]
<key-string>

no atmf virtual-link id <1-4094> protection
```

| Parameter    | Description   |
|--------------|---|
| id           | Specify the link ID.  |
| <1-4094>     | Link ID in the range 1 to 4094,   |
| protection   | Protection is on for this link.   |
| ipsec        | Security provided using IPsec.  |
| key          | Set the shared key.   |
| 8            | Specifies a string in an encrypted format instead of plain text. The running config will display the new password as an encrypted string even if password encryption is turned off. |
| <key-string> | Specify the shared key for the link.  |

**Default** Protection is off by default.

**Mode** Global Configuration

**Usage notes** The following limitations need to be considered when creating secure virtual-links.

- Switch devices support a maximum of 20 downstream AMF nodes when using a secure virtual-link as an uplink.
- When there are two or more AMF members behind a shared NAT device, only one of the members will be able to use secure virtual-links.
- An AMF Multi-tenant environment supports a maximum cumulative total of 1200 secure virtual-links across all AMF containers.

Secure virtual-links are only supported on the following device listed in the table below. There is also a limit to the number of links these devices support.

| Device  | Virtual-link Limit |
|---|--------------------|
| AMF Cloud/ VAA  | 300                |
| AR4050S<br>AR3050S<br>AR2050V<br>AR2010V              | 60                 |
| x220<br>x230/x230L<br>x310<br>x510/x510L<br>IX5-28GPX | 2                  |

**Example** To create and configure a virtual link with protection first create the virtual-link:

```
Host-A# configure terminal
```

```
Host-A(config)# atmf virtual-link id 1 ip 192.168.1.1 remote-id  
2 remote-ip 192.168.2.1
```

Enable protection on the virtual link:

```
Host-A(config)# atmf virtual-link id 1 protection ipsec key  
securepassword
```

Repeat these steps on the other side of the link:

```
Host-B(config)# atmf virtual-link id 2 ip 192.168.2.1 remote-id  
1 remote-ip 192.168.1.1
```

```
Host-B(config)# atmf virtual-link id 2 protection ipsec key  
securepassword
```

**Related  
commands** [atmf virtual-link](#)

[show atmf](#)

[show atmf links](#)

[show atmf virtual-links](#)

**Command  
changes** Version 5.4.9-0.1: command added

# atmf working-set

**Overview** Use this command to execute commands across an individually listed set of AMF nodes or across a named group of nodes.

Note that this command can only be run on a master node.

Use the **no** variant of this command to remove members or groups from the current working-set.

**Syntax** `atmf working-set { [<node-list> ] | [group <group-list> | all | local | current] }`  
`no atmf working-set { [<node-list> ] | [group <group-list> ] }`

| Parameter                       | Description  |
|---------------------------------|--|
| <code>&lt;node-list&gt;</code>  | A comma delimited list (without spaces) of nodes to be included in the working-set.  |
| <code>group</code>              | The AMF group.   |
| <code>&lt;group-list&gt;</code> | 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. |
| <code>all</code>                | All nodes in the AMF.  |
| <code>local</code>              | Local node<br>Running this command with the parameters <b>group local</b> will return you to the local prompt and local node connectivity.   |
| <code>current</code>            | Nodes in current list.   |

**Mode** Privileged Exec

**Usage notes** You can put AMF nodes into groups by using the [atmf group \(membership\)](#) command.

This command opens a session on multiple network devices. When you change the working set to anything other than the local device, the prompt will change to the AMF network name, followed by the size of the working set, shown in square brackets. This command has to be run at privilege level 15.

In addition to the user defined groups, the following system assigned groups are automatically created:

- Implicit Groups
  - local: The originating node.
  - current: All nodes that comprise the current working-set.
  - all: All nodes in the AMF.

- Automatic Groups - These can be defined by hardware architecture, e.g. x510, x610, x8100, AR3050S or AR4050S, or by certain AMF nodal designations such as master.

Note that the Implicit Groups do not appear in `show atmf group` command output. If a node is an AMF master it will be automatically added to the master group.

**Example 1** To add all nodes in the AMF to the working-set, use the command:

```
node1# atmf working-set group all
```

**NOTE:** This command adds the implicit group "all" to the working set, where "all" comprises all nodes in the AMF.

This command displays an output screen similar to the one shown below:

```
=====
node1, node2, node3, node4, node5, node6:
=====

Working set join

ATMF_NETWORK_Name[6]#
```

**Example 2** To return to the local prompt, and connect to only the local node, use the command:

```
ATMF_Network_Name[6]# atmf working-set group local
node1#
```

The following table describes the meaning of the prompts in this example.

| Parameter         | Description  |
|-------------------|--|
| ATMF_Network_Name | The name of the AMF network, as set by the <code>atmf network-name</code> command. |
| [ 6 ]             | The number of nodes in the working-set.  |
| node1             | The name of the local node, as set by the <code>hostname</code> command.           |

# bridge-group

**Overview** Use this command to connect an AMF container to a bridge created on a Virtual AMF Appliance (VAA) virtual machine. This allows the AMF container to connect to a physical network.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove a bridge-group from an AMF container.

**Syntax** `bridge-group <bridge-id>`  
`no bridge-group`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;bridge-id&gt;</code> | The ID of the bridge group to join, a number between 1 and 64. |

**Mode** AMF Container Configuration

**Usage notes** Each container has two virtual interfaces:

- 1) Interface eth0, used to connect to the AMF controller on the VAA host via an AMF area-link, and configured using this [area-link](#) command.
- 2) Interface eth1, used to connect to the outside world using a bridged L2 network link, and configured using the **bridge-group** command.

Before using this command, a bridge must be created with the same bridge-id on the VAA host using the **bridge <bridge-id>** command.

See the [AMF Feature Overview and Configuration Guide](#) for more information on configuring the bridge.

**Example** To create a bridge group for AMF container "vac-wlg-1" and , use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# bridge-group 1
```

**Related commands** [atmf container](#)  
[show atmf container](#)

**Command changes** Version 5.4.7-0.1: command added

# clear application-proxy threat-protection

**Overview** Use this command to clear the threat protection for a specified address.

**Syntax** `clear application-proxy threat-protection {<ip-address>|<mac-address>|all}`

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;ip-address&gt;</code>  | The IPv4 address you wish to clear the threat for, in A.B.C.D format.       |
| <code>&lt;mac-address&gt;</code> | The MAC address you wish to clear the threat for, in HHHH.HHHH.HHHH format. |
| <code>all</code>                 | Clear the threat for all IPv4 and MAC addresses.                            |

**Mode** Privileged Exec

**Example** To clear the threat for 10.34.199.117, use the command:

```
awplus# clear application-proxy threat-protection 10.34.199.117
```

**Related commands**

- [application-proxy quarantine-vlan](#)
- [application-proxy threat-protection](#)
- [application-proxy threat-protection send-summary](#)
- [service atmf-application-proxy](#)
- [show application-proxy threat-protection](#)

**Command changes** Version 5.4.7-2.2: command added

# clear atmf links

**Overview** Use this command with no parameters to manually reset all the AMF links on a device. You can optionally specify an interface or range of interfaces to reset the links on.

Certain events or topology changes can cause AMF links to be incorrect or outdated. Clearing the links forces AMF to relearn the information from neighboring nodes and create a fresh, correct, view of the network.

**Syntax** `clear atmf links [<interface-list>]`

| Parameter                           | Description   |
|-------------------------------------|---|
| <code>&lt;interface-list&gt;</code> | <p>The interfaces or ports to perform the reset on. An interface-list can be:</p> <ul style="list-style-type: none"><li>• a switchport (e.g. port1.0.1)</li><li>• a static channel group (e.g. sa2)</li><li>• a dynamic (LACP) channel group (e.g. po2)</li><li>• a local port (e.g. of0)</li><li>• You can specify a continuous range of interfaces separated by a hyphen, or a comma-separated list (e.g. port1.0.1, port1.0.4-port1.0.18).</li></ul> <p>The specified interfaces must exist.<br/>If this parameter is left out then all links of the specified type will be reset on the device.</p> |

**Mode** Privileged Exec

**Example** To clear all AMF links on a device, use the following command:

```
awplus# clear atmf links
```

To clear all AMF links on port1.0.1 to port1.0.4 and static aggregator sa1, use the following command:

```
awplus# clear atmf links port1.0.1-port1.0.4,sa1
```

**Related commands** [clear atmf links virtual](#)  
[show atmf links](#)

**Command changes** Version 5.4.8-2.1: command added



# clear atmf links virtual

**Overview** Use this command with no parameters to manually reset all the AMF virtual links on a device. You can, optionally, specify a comma separated list of virtual links to reset.

Certain events or topology changes can cause AMF links to be incorrect or outdated. Clearing the links forces AMF to relearn the information from neighboring nodes and create a fresh, correct view of the network.

**Syntax** `clear atmf links virtual [<virtuallink-list>]`

| Parameter                             | Description  |
|---------------------------------------|--|
| <code>&lt;virtuallink-list&gt;</code> | A single, or list, of AMF virtual link identifiers to reset. This must be a comma separated list of links e.g. <code>vlink1, vlink2, vlink3</code> . Specifying a link range e.g. <code>vlink1-vlink3</code> is not supported. |

**Mode** Privileged Exec

**Example** To clear all AMF virtual links on a device, use the following command:

```
awplus# clear atmf links virtual
```

To clear AMF virtual links `vlink11` and `vlink21`, use the following command:

```
awplus# clear atmf links virtual vlink11,vlink22
```

**Related commands** [clear atmf links](#)  
[show atmf links](#)

**Command changes** Version 5.4.8-2.1: command added

# clear atmf links statistics

**Overview** This command resets the values of all AMF link, port, and global statistics to zero.

**Syntax** `clear atmf links statistics`

**Mode** Privilege Exec

**Example** To reset the AMF link statistics values, use the command:

```
node_1# clear atmf links statistics
```

**Related commands** [show atmf links statistics](#)

# clear atmf recovery-file

**Overview** Use this command to delete all of a node's recovery files. It deletes the recovery files stored on:

- the local node,
- neighbor nodes, and
- external media (USB or SD card).

**Syntax** `clear atmf recovery-file`

**Mode** Privileged Exec

**Usage notes** AMF recovery files are created for nodes with special links. Special links include:

- virtual links,
- area links terminating on an AMF master, and
- area virtual links terminating on an AMF master.

An AMF node with one of these special links pushes its startup configuration to its neighbors and to any attached external media. It then fetches and applies this configuration at recovery time. This configuration enables it to contact the AMF master and initiate a recovery.

Recovery files can become out of date if:

- a node's neighbor is off line when changes are made to its configuration, or
- when a node no longer contains a special link.

**Example** To clear a node's recovery files, use the command:

```
node1# clear atmf recovery-file
```

**Output** Figure 19-2: If AlliedWare Plus detects that a node contains a special link then the following message is displayed

```
node1#clear atmf recovery-file
% Warning: ATMF recovery files have been removed.
ATMF recovery may fail. Please save running-configuration.
```

**Related commands** [show atmf recovery-file](#)

**Command changes** Version 5.4.8-0.2: command added

# clear atmf secure-mode certificates

**Overview** Use this command to remove all certificates from an AMF member or master. AMF nodes will need to be re-authorized once this command has been run.

**Syntax** `clear atmf secure-mode certificates`

**Mode** Privileged Exec

**Example** To clear all certificates from an AMF node, use the command:

```
awplus# clear atmf secure-mode certificates
```

If this is the only master on the network you will see the following warning:

```
% Warning: This node is the only master in the network!  
All the nodes will become isolated and refuse to join any ATMF  
network. The certificates on all the isolated nodes must be  
cleared before rejoining an ATMF network will be possible.  
  
To clear certificates a reboot of the device is required.  
Clear certificates and Reboot ? (y/n):
```

On an AMF member you will see the following message:

```
To clear certificates a reboot of the device is required.  
Clear certificates and Reboot ? (y/n):
```

**Related commands**

- [atmf authorize](#)
- [atmf secure-mode](#)
- [show atmf authorization](#)
- [show atmf secure-mode certificates](#)

**Command changes** Version 5.4.7-0.3: command added

# clear atmf secure-mode statistics

**Overview** Use this command to reset all secure mode statistics to 0.

**Syntax** `clear atmf secure-mode statistics`

**Mode** Privileged Exec

**Example** To reset the AMF secure mode statistics information, use the command:

```
awplus# clear atmf secure-mode statistic
```

**Related commands** [show atmf secure-mode](#)  
[show atmf secure-mode statistics](#)

**Command changes** Version 5.4.7-0.3: command added

# clone (amf-provision)

**Overview** This command sets up a space on the backup media for use with a provisioned node and copies into it almost all files and directories from a chosen backup or provisioned node.

Alternatively, you can set up a new, unique provisioned node by using the command [create \(amf-provision\)](#).

**Syntax** `clone <source-nodename>`

| Parameter                            | Description  |
|--------------------------------------|--|
| <code>&lt;source-nodename&gt;</code> | The name of the node whose configuration is to be copied for loading to the clone. |

**Mode** AMF Provisioning

**Usage notes** This command is only available on master nodes in the AMF network.

When using this command it is important to be aware of the following:

- A copy of `<media>:atmf/<atmf_name>/nodes/<source_node>/flash` will be made for the provisioned node and stored in the backup media.
- The directory `<node_backup_dir>/flash/.config/ssh` is excluded from the copy.
- All contents of `<root_backup_dir>/nodes/<nodename>` will be deleted or overwritten.
- Settings for the expected location of other provisioned nodes are excluded from the copy.

The active and backup configuration files are automatically modified in the following ways:

- The **hostname** command is modified to match the name of the provisioned node.
- The **stack virtual-chassis-id** command is removed, if present.

**Example** To copy from the backup of 'device2' to create backup files for the new provisioned node 'device3' use the following command:

```
device1# atmf provision node device3  
device1(atmf-provision)# clone device2
```

Figure 19-3: Sample output from the **clone** command

```
device1# atmf provision node device3  
device1(atmf-provision)# clone device2  
Copying...  
Successful operation
```

To confirm that a new provisioned node has been cloned, use the command:

```
device1# show atmf backup
```

The output from this command is shown in the following figure, and shows the details of the new provisioned node 'device3'.

Figure 19-4: Sample output from the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup ..... Enabled
  Schedule ..... 1 per day starting at 03:00
  Next Backup Time ... 01 Oct 2018 03:00
Backup Bandwidth ..... Unlimited
Backup Media ..... USB (Total 7446.0MB, Free 7297.0MB)
Server Config .....
  Synchronization .... Unsynchronized
  Last Run ..... -
  1 ..... Unconfigured
  2 ..... Unconfigured
Current Action ..... Idle
Started ..... -
Current Node ..... -

-----
Node Name      Date           Time           In ATMF  On Media  Status
-----
device3        -              -              No       Yes       Prov
device1        30 Sep 2018   00:05:49      No       Yes       Good
device2        30 Sep 2018   00:05:44      Yes      Yes       Good
```

**Related commands**

- atmf provision (interface)
- atmf provision node
- configure boot config (amf-provision)
- configure boot system (amf-provision)
- copy (amf-provision)
- create (amf-provision)
- delete (amf-provision)
- identity (amf-provision)
- license-cert (amf-provision)
- locate (amf-provision)
- show atmf provision nodes

**Command changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# configure boot config (amf-provision)

**Overview** This command sets the configuration file to use during the next boot cycle. This command can also set a backup configuration file to use if the main configuration file cannot be accessed for an AMF provisioned node. To unset the boot configuration or the backup boot configuration use the **no boot** command.

**Syntax** `configure boot config [backup] <file-path|URL>`  
`configure no boot config [backup]`

| Parameter       | Description   |
|-----------------|---|
| backup          | Specify that this is the backup configuration file. |
| <file-path URL> | The path or URL and name of the configuration file. |

**Default** No boot configuration files or backup configuration files are specified for the provisioned node.

**Mode** AMF Provisioning

**Usage notes** When using this command to set a backup configuration file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

**Examples** To set the configuration file 'branch.cfg' on the AMF provisioned node 'node1', use the command:

```
MasterNodeName# atmf provision node node1
MasterNodeName(atmf-provision)# configure boot config
branch.cfg
```

To set the configuration file 'backup.cfg' as the backup to the main configuration file on the AMF provisioned node 'node1', use the command:

```
MasterNodeName(atmf-provision)# configure boot config backup
usb:/atmf/amf_net/nodes/node1/config/backup.cfg
```

To unset the boot configuration, use the command:

```
MasterNodeName(atmf-provision)# configure no boot config
```

To unset the backup boot configuration, use the command:

```
MasterNodeName(atmf-provision)# configure no boot config backup
```

**Related commands**

- [atmf provision \(interface\)](#)
- [atmf provision node](#)
- [clone \(amf-provision\)](#)
- [configure boot system \(amf-provision\)](#)
- [create \(amf-provision\)](#)



delete (amf-provision)  
identity (amf-provision)  
license-cert (amf-provision)  
locate (amf-provision)  
show atmf provision nodes

**Command  
changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# configure boot system (amf-provision)

**Overview** This command sets the release file that will load onto a specified provisioned node during the next boot cycle. This command can also set the backup release file to be loaded for an AMF provisioned node. To unset the boot system release file or the backup boot release file use the **no boot** command.

Use the **no** variant of this command to return to the default.

This command can only be run on AMF master nodes.

**Syntax** `configure boot system [backup] <file-path|URL>`  
`configure no boot system [backup]`

| Parameter                          | Description                                   |
|------------------------------------|---|
| <code>&lt;file-path URL&gt;</code> | The path or URL and name of the release file. |

**Default** No boot release file or backup release files are specified for the provisioned node.

**Mode** AMF Provisioning

**Usage notes** When using this command to set a backup release file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

**Examples** To set the release file x930-5.4.9-0.1.rel on the AMF provisioned node 'node1', use the command:

```
MasterNodeName# atmf provision node node1
MasterNodeName(atmf-provision)# configure boot system
x930-5.4.9-0.1.rel
```

To set the backup release file x930-5.4.8-2.5.rel as the backup to the main release file on the AMF provisioned node 'node1', use the command:

```
MasterNodeName# atmf provision node node1
MasterNodeName(atmf-provision)# configure boot system backup
card:/atmf/amf_net/nodes/node1/flash/x930-5.4.8-2.5.rel
```

To unset the boot release, use the command:

```
MasterNodeName# atmf provision node node1
MasterNodeName(atmf-provision)# configure no boot system
```

To unset the backup boot release, use the command:

```
MasterNodeName# atmf provision node node1
MasterNodeName(atmf-provision)# configure no boot system backup
```

**Related commands** [atmf provision \(interface\)](#)

atmf provision node  
clone (amf-provision)  
configure boot config (amf-provision)  
create (amf-provision)  
delete (amf-provision)  
identity (amf-provision)  
license-cert (amf-provision)  
locate (amf-provision)  
show atmf provision nodes

**Command  
changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# copy (amf-provision)

**Overview** Use this command to copy configuration and release files for the node you are provisioning.

For more information about using the copy command see [copy \(filename\)](#) in the File and Configuration Management chapter.

**Syntax** `copy [force] <source-name> <destination-name>`

| Parameter                             | Description   |
|---------------------------------------|---|
| <code>force</code>                    | This parameter forces the copy command to overwrite the destination file, if it already exists, without prompting the user for confirmation.        |
| <code>&lt;source-name&gt;</code>      | The filename and path of the source file. See the <a href="#">Introduction</a> of the File and Configuration Management chapter for valid syntax.   |
| <code>&lt;destination-name&gt;</code> | The filename and path for the destination file. See <a href="#">Introduction</a> of the File and Configuration Management chapter for valid syntax. |

**Mode** AMF Provisioning

**Example** To copy a configuration file named `current.cfg` from Node\_4's Flash into the `future_node` directory, and set that configuration file to load onto `future_node`, use the following commands:

```
node_4# atmf provision node future_node
node_4(atmf-provision)# create
node_4(atmf-provision)# locate
node_4(atmf-provision)# copy flash:current.cfg
./future_node.cfg
node_4(atmf-provision)# configure boot config future_node.cfg
```

**Related commands**

- [atmf provision \(interface\)](#)
- [atmf provision node](#)
- [clone \(amf-provision\)](#)
- [create \(amf-provision\)](#)
- [delete \(amf-provision\)](#)
- [locate \(amf-provision\)](#)
- [show atmf provision nodes](#)

**Command changes** Version 5.4.9-2.1: command added

# create (amf-provision)

**Overview** This command sets up an empty directory on the backup media for use with a provisioned node. This directory can have configuration and release files copied to it from existing devices. Alternatively, the configuration files can be created by the user.

An alternative way to create a new provisioned node is with the command [clone \(amf-provision\)](#).

This command can only run on AMF master nodes.

**Syntax** create

**Mode** AMF Provisioning

**Usage notes** This command is only available on master nodes in the AMF network.

A date and time is assigned to the new provisioning directory reflecting when this command was executed. If there is a backup or provisioned node with the same name on another AMF master then the most recent one will be used.

**Example** To create a new provisioned node named "device2" use the command:

```
device1# atmf provision node device2  
device1(atmf-provision)# create
```

Running this command will create the following directories:

- `<media>:atmf/<atmf_name>/nodes/<node>`
- `<media>:atmf/<atmf_name>/nodes/<node>/flash`

To confirm the new node's settings, use the command:

```
device1# show atmf backup
```

The output for the **show atmf backup** command is shown in the following figure, and shows details for the new provisioned node 'device2'.

Figure 19-5: Sample output from the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup ..... Enabled
  Schedule ..... 1 per day starting at 03:00
  Next Backup Time .... 01 Oct 2018 03:00
Backup Bandwidth ..... Unlimited
Backup Media ..... USB (Total 7446.0MB, Free 7315.2MB)
Server Config .....
  Synchronization ..... Unsynchronized
  Last Run ..... -
  1 ..... Unconfigured
  2 ..... Unconfigured
Current Action ..... Idle
  Started ..... -
  Current Node ..... -

-----
Node Name      Date           Time           In ATMF  On Media  Status
-----
device2        -              -              No        Yes       Prov
device1        30 Sep 2018   00:05:49      No        Yes       Good
```

For instructions on how to configure on a provisioned node, see the [AMF Feature Overview and Configuration Guide](#).

**Related commands**

- [atmf provision \(interface\)](#)
- [atmf provision node](#)
- [clone \(amf-provision\)](#)
- [copy \(amf-provision\)](#)
- [configure boot config \(amf-provision\)](#)
- [configure boot system \(amf-provision\)](#)
- [delete \(amf-provision\)](#)
- [identity \(amf-provision\)](#)
- [license-cert \(amf-provision\)](#)
- [locate \(amf-provision\)](#)
- [show atmf provision nodes](#)

**Command changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# debug atmf

**Overview** This command enables the AMF debugging facilities, and displays information that is relevant (only) to the current node. The detail of the debugging displayed depends on the parameters specified.

If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

The **no** variant of this command disables either all AMF debugging information, or only the particular information as selected by the command's parameters.

**Syntax**

```
debug atmf  
[link | crosslink | arealink | database | neighbor | error | all]  
  
no debug atmf  
[link | crosslink | arealink | database | neighbor | error | all]
```

| Parameter | Description   |
|-----------|---|
| link      | Output displays debugging information relating to uplink or downlink information. |
| crosslink | Output displays all crosslink events.   |
| arealink  | Output displays all arealink events.  |
| database  | Output displays only notable database events.                                     |
| neighbor  | Output displays only notable AMF neighbor events.                                 |
| error     | Output displays AMF error events.   |
| all       | Output displays all AMF events.   |

**Default** All debugging facilities are disabled.

**Mode** User Exec and Global Configuration

**Usage notes** If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

**NOTE:** An alias to the **no** variant of this command is [undebg atmf](#) on page 896.

**Examples** To enable all AMF debugging, use the command:

```
node_1# debug atmf
```

To enable AMF uplink and downlink debugging, use the command:

```
node_1# debug atmf link
```

To enable AMF error debugging, use the command:

```
node_1# debug atmf error
```

**Related** [no debug all](#)  
**commands**



# debug atmf packet

**Overview** This command configures AMF Packet debugging parameters. The debug only displays information relevant to the current node. The command has following parameters:

**Syntax** debug atmf packet [direction {rx|tx|both}] [level {1|2|3}]  
[timeout <seconds>] [num-pkts <quantity>]  
[filter {node <name>|interface <ifname>}]  
[pkt-type [1][2][3][4][5][6][7][8][9][10][11][12][13]]

## Simplified Syntax

|                          |   |
|--------------------------|---|
| debug atmf packet        | [direction {rx tx both}]                                  |
|                          | [level {[1][2][3]}]                                       |
|                          | [timeout <seconds>]                                       |
|                          | [num-pkts <quantity>]                                     |
| debug atmf packet filter | [node <name>]   |
|                          | [interface <ifname>]                                      |
|                          | [pkt-type<br>[1][2][3][4][5][6][7][8][9][10][11][12][13]] |

**NOTE:** You can combine the syntax components shown, but when doing so, you must retain their original order.

**Default** Level 1, both Tx and Rx, a timeout of 60 seconds with no filters applied.

**NOTE:** An alias to the **no** variant of this command - *undebug atmf* - can be found elsewhere in this chapter.

**Mode** User Exec and Global Configuration

**Usage notes** If no additional parameters are specified, then the command output will apply a default selection of parameters shown below:

| Parameter | Description  |
|-----------|--|
| direction | Sets debug to packet received, transmitted, or both  |
| rx        | packets received by this node  |
| tx        | Packets sent from this node  |
| 1         | AMF Packet Control header Information, Packet Sequence Number. Enter 1 to select this level. |
| 2         | AMF Detailed Packet Information. Enter 2 to select this level.                               |
| 3         | AMF Packet HEX dump. Enter 3 to select this level.   |
| timeout   | Sets the execution timeout for packet logging  |

| Parameter  | Description   |
|------------|---|
| <seconds>  | Seconds   |
| num-pkts   | Sets the number of packets to be dumped   |
| <quantity> | The actual number of packets  |
| filter     | Sets debug to filter packets  |
| node       | Sets the filter on packets for a particular Node  |
| <name>     | The name of the remote node   |
| interface  | Sets the filter to dump packets from an interface (portx.x.x) on the local node                   |
| <ifname>   | Interface port or virtual-link  |
| pkt-type   | Sets the filter on packets with a particular AMF packet type                                      |
| 1          | Crosslink Hello BPDU packet with crosslink links information. Enter 1 to select this packet type. |
| 2          | Crosslink Hello BPDU packet with downlink domain information. Enter 2 to select this packet type. |
| 3          | Crosslink Hello BPDU packet with uplink information. Enter 3 to select this packet type.          |
| 4          | Downlink and uplink hello BPDU packets. Enter 4 to select this packet type.                       |
| 5          | Non broadcast hello unicast packets. Enter 5 to select this packet type.                          |
| 6          | Stack hello unicast packets. Enter 6 to select this packet type.                                  |
| 7          | Database description. Enter 7 to select this packet type.   |
| 8          | DBE request. Enter 8 to select this packet type.  |
| 9          | DBE update. Enter 9 to select this packet type.   |
| 10         | DBE bitmap update. Enter 10 to select this packet type.   |
| 11         | DBE acknowledgment. Enter 11 to select this packet type.  |
| 12         | Area Hello Packets. Enter 12 to select this packet type.  |
| 13         | Gateway Hello Packets. Enter 13 to select this packet type.                                       |

**Examples** To set a packet debug on node 1 with level 1 and no timeout, use the command:

```
node_1# debug atmf packet direction tx timeout 0
```

To set a packet debug with level 3 and filter packets received from AMF node 1:

```
node_1# debug atmf packet direction tx level 3 filter node_1
```

To enable send and receive 500 packets only on vlink1 for packet types 1, 7, and 11, use the command:

```
node_1# debug atmf packet num-pkts 500 filter interface vlink1  
pkt-type 1 7 11
```

This example applies the **debug atmf packet** command and combines many of its options:

```
node_1# debug atmf packet direction rx level 1 num-pkts 60  
filter node x930 interface port1.0.1 pkt-type 4 7 10
```

# delete (amf-provision)

**Overview** This command deletes files that have been created for loading onto a provisioned node. It can only be run on master nodes.

**Syntax** delete

**Mode** AMF Provisioning

**Usage notes** This command is only available on master nodes in the AMF network. The command will only work if the provisioned node specified in the command has already been set up (although the device itself is still yet to be installed). Otherwise, an error message is shown when the command is run.

You may want to use the **delete** command to delete a provisioned node that was created in error or that is no longer needed.

This command cannot be used to delete backups created by the AMF backup procedure. In this case, use the command [atmf backup delete](#) to delete the files.

**NOTE:** *This command allows provisioned entries to be deleted even if they have been referenced by the [atmf provision \(interface\)](#) command, so take care to only delete unwanted entries.*

**Example** To delete backup files for a provisioned node named device3 use the command:

```
device1# atmf provision node device3  
device1(atmf-provision)# delete
```

To confirm that the backup files for provisioned node device3 have been deleted use the command:

```
device1# show atmf backup
```

The output should show that the provisioned node device3 no longer exists in the backup file, as shown in the figure below:

Figure 19-6: Sample output showing the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup ..... Enabled
  Schedule ..... 1 per day starting at 03:00
  Next Backup Time .... 01 Oct 2016 03:00
Backup Bandwidth ..... Unlimited
Backup Media ..... USB (Total 7446.0MB, Free 7297.0MB)
Server Config .....
  Synchronization .... Unsynchronized
  Last Run ..... -
  1 ..... Unconfigured
  2 ..... Unconfigured
Current Action ..... Idle
  Started ..... -
  Current Node ..... -

-----
Node Name      Date           Time           In ATMF  On Media  Status
-----
device1        30 Sep 2016   00:05:49      No       Yes       Good
device2        30 Sep 2016   00:05:44      Yes      Yes       Good
```

**Related commands**

- atmf provision (interface)
- atmf provision node
- clone (amf-provision)
- configure boot config (amf-provision)
- configure boot system (amf-provision)
- create (amf-provision)
- identity (amf-provision)
- license-cert (amf-provision)
- locate (amf-provision)
- show atmf provision nodes

**Command changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# discovery

**Overview** Use this command to specify how AMF learns about guest nodes.

AMF nodes gather information about guest nodes by using one of two internally defined discovery methods: static or dynamic.

With dynamic learning (the default method), AMF learns IP address and MAC addresses of guest nodes from LLDP or DHCP snooping. Dynamic learning is only supported when using IPv4. For IPv6, use static learning.

With static learning, you use the `switchport atmf-guestlink` command to specify the guest class name and IP address of the guest node attached to each individual switch port. AMF then learns the MAC addresses of each of the guests of that class from ARP or Neighbor discovery tables.

If you are using the static method, ensure that you have configured the appropriate class type for each of your statically discovered guest nodes.

The **no** variant of this command returns the discovery method to **dynamic**.

**Syntax** `discovery [static|dynamic]`  
`no discovery`

| Parameter            | Description                          |
|----------------------|--------------------------------------|
| <code>static</code>  | Statically assigned.                 |
| <code>dynamic</code> | Learned from DCHCP Snooping or LLDP. |

**Default** Dynamic.

**Mode** ATMF Guest Configuration Mode.

**Usage notes** This command is one of several modal commands that are configured and applied for a specific guest-class (mode). Its settings are automatically applied to a guest-node link by the `switchport atmf-guestlink` command.

**NOTE:** *AMF guest nodes are not supported on ports using the OpenFlow protocol.*

**Example 1** To configure the discovery of the guest-class camera to operate statically, use the following commands:

```
Node1# configure terminal
Node1(config)# atmf guest-class camera
Node1(config-guest)# discovery static
```

**Example 2** To return the discovery method for the guest class TQ4600-1 to its default of **dynamic**, use the following commands:

```
Node1# configure terminal
Node1(config)# atmf guest-class TQ4600-1
Node1(config-guest)# no discovery
```

**Related commands**

- atmf guest-class
- switchport atmf-guestlink
- show atmf links guest
- show atmf nodes

# description (amf-container)

**Overview** Use this command to set the description on an AMF container on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove the description from an AMF container.

**Syntax** `description <description>`  
`no description`

| Parameter                        | Description  |
|----------------------------------|--|
| <code>&lt;description&gt;</code> | Enter up to 128 characters of text describing the AMF container. |

**Mode** AMF Container Configuration

**Example** To set the description for AMF container “vac-wlg-1” to “Wellington area”, use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# description Wellington area
```

To remove the description for AMF container “vac-wlg-1”, use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# no description
```

**Related commands** [atmf container](#)  
[show atmf container](#)

**Command changes** Version 5.4.7-0.1: command added



# erase factory-default

**Overview** This command erases all data from NVS and all data from Flash **except** the following:

- the boot release file (a .rel file) and its release setting file
- all license files
- the latest GUI release file

The device is then rebooted and returned to its factory default condition. The device can then be used for AMF automatic node recovery.

**Syntax** `erase factory-default`

**Mode** Privileged Exec.

**Usage notes** This command is an alias to the [atmf cleanup](#) command.

**Example** To erase data, use the command:

```
Node_1# erase factory-default
```

```
This command will erase all NVS, all flash contents except for  
the boot release, a GUI resource file, and any license files,  
and then reboot the switch. Continue? (y/n):y
```

**Related commands** [atmf cleanup](#)

# http-enable

**Overview** This command is used to enable GUI access to a guest node. When http-enable is configured the port number is set to its default of 80. If the guest node is using a different port for HTTP, you can configure this using the port <PORTNO> attribute.

This command is used to inform the GUI that this device has an HTTP interface at the specified port number so that a suitable URL can be provided to the user.

Use the **no** variant of this command to disable HTTP.

**Syntax** http-enable [port <port-number>]  
no http-enable

| Parameter     | Description                       |
|---------------|-----------------------------------|
| port          | TCP port number.                  |
| <port-number> | The port number to be configured. |

**Default** http-enable is off.  
If http-enable is selected without a port parameter the port number will default to 80.

**Mode** ATMF Guest Configuration Mode

**Example 1** To enable HTTP access to a guest node on port 80 (the default), use the following commands:

```
node1# conf t
node1(config)#atmf guest-class Camera
node1(config-atmf-guest)#http-enable
node1(config-atmf-guest)#
```

**Example 2** To enable HTTP access to a guest node on port 400, use the following commands:

```
node1# conf t
node1(config)#atmf guest-class Camera
node1(config-atmf-guest)#http-enable port 400
node1(config-atmf-guest)#
```

**Example 3** To disable HTTP access to a guest node, use the following commands:

```
node1# conf t
node1(config)#atmf guest-class Camera
node1(config-atmf-guest)#no http-enable
node1(config-atmf-guest)#
```

**Related  
commands**    `atmf guest-class`  
                  `switchport atmf-guestlink`  
                  `show atmf links guest`  
                  `show atmf nodes`

# identity (amf-provision)

**Overview** Use this command to create an identity token for provisioning an isolated AMF node. An isolated node is an AMF member that is only connected to the rest of the AMF network via a virtual-link.

This command allows these nodes, which have no AMF neighbors, to be identified for provisioning purposes. They are identified using an identity token which is based on either the next-hop MAC address of the provisioned node, or the serial number of the device being provisioned. This identity token is stored on the AMF master.

Use the **no** variant of this command to remove the identity token for a node.

**Syntax**

```
identity mac-address <mac-address> prefix  
<ip-address/prefix-length>  
  
identity serial-number <serial-number> prefix  
<ip-address/prefix-length>  
  
no identity
```

| Parameter                      | Description   |
|--------------------------------|---|
| mac-address                    | Specify the next-hop MAC address of the device being provisioned.                           |
| <mac-address>                  | MAC address of the port the provisioned node is connected to, in the format xxxx.xxxx.xxxx. |
| serial-number                  | Specify the serial number of the device to be provisioned.                                  |
| <serial-number>                | Serial number of the device that is being provisioned.                                      |
| prefix                         | IPv4 address, and prefix length, of the virtual-link interface on the isolated node         |
| <ip-address/<br>prefix-length> | IPv4 address, and prefix length, in A.B.C.D/M format.                                       |

**Mode** AMF Provisioning

**Usage notes** To provision an isolated node, first create a configuration for the node using the [create \(amf-provision\)](#) and/or the [clone \(amf-provision\)](#) commands.

Then create an identity token for the provisioned node by either specifying its next-hop MAC address or by specifying the serial number of the replacement device. The advantage of using the next-hop MAC address is that any device, regardless of its serial number, can be added to the network but using the serial number maybe preferred in situations where the next-hop MAC address is not easy to obtain.

The [atmf recovery-server](#) option must be enabled on the AMF master before attempting to provision the device. This option allows the AMF master to process recovery requests from isolated AMF nodes.

See the [AMF Feature Overview and Configuration Guide](#) for information on preparing your network for recovering or provisioning isolated nodes.

**Example** To create a identity token on your AMF master for a device named “my-x930” with serial number “A10064A172100008”, use the command:

```
awplus# atmf provision node my-x930  
awplus(atmf-provision)# identity serial-number  
A10064A172100008 prefix 192.168.2.25/24
```

To create a identity token on your AMF master for a device named “my-x930” with next-hop MAC address “0000.cd28.0880”, use the command:

```
awplus# atmf provision node my-x930  
awplus(atmf-provision)# identity mac-address 0000.cd28.0880  
prefix 192.168.2.25/24
```

To delete the identity token from your AMF master for a device named “my-x930”, use the command:

```
awplus# atmf provision node my-x930  
awplus(atmf-provision)# no identity
```

**Related  
commands**

[atmf cleanup](#)  
[atmf provision \(interface\)](#)  
[atmf provision node](#)  
[atmf recovery-server](#)  
[atmf virtual-link](#)  
[clone \(amf-provision\)](#)  
[configure boot config \(amf-provision\)](#)  
[configure boot system \(amf-provision\)](#)  
[create \(amf-provision\)](#)  
[delete \(amf-provision\)](#)  
[license-cert \(amf-provision\)](#)  
[locate \(amf-provision\)](#)  
[show atmf provision nodes](#)

**Command  
changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode  
Version 5.4.7-2.1: command added

# license-cert (amf-provision)

**Overview** This command is used to set up the license certificate for a provisioned node.

The certificate file usually has all the license details for the network, and can be stored anywhere in the network. This command makes a hidden copy of the certificate file and stores it in the space set up for the provisioned node on AMF backup media.

For node provisioning, the new device has not yet been part of the AMF network, so the user is unlikely to know its product ID or its MAC address. When such a device joins the network, assuming that this command has been applied successfully, the copy of the certificate file will be applied automatically to the provisioned node.

Once the new device has been resurrected on the network and the certificate file has been downloaded to the provisioned node, the hidden copy of the certificate file is deleted from AMF backup media.

Use the **no** variant of this command to set it back to the default.

This command can only be run on AMF master nodes.

**Syntax** `license-cert <file-path/URL>`  
`no license-cert`

| Parameter                          | Description   |
|------------------------------------|---|
| <code>&lt;file-path/URL&gt;</code> | The name of the certificate file. This can include the file-path of the file. |

**Default** No license certificate file is specified for the provisioned node.

**Mode** AMF Provisioning

**Usage notes** This command is only available on master nodes in the AMF network. It will only operate if the provisioned node specified in the command has already been set up, and if the license certification is present in the backup file. Otherwise, an error message is shown when the command is run.

**Example 1** To apply the license certificate 'cert1.txt' stored on a TFTP server for AMF provisioned node "device2", use the command:

```
device1# atmf provision node device2
device1(atmf-provision)# license-cert
tftp://192.168.1.1/cert1.txt
```

**Example 2** To apply the license certificate 'cert2.txt' stored in the AMF master's flash directory for AMF provisioned node 'host2', use the command:

```
device1# atmf provision node host2
device1(atmf-provision)# license-cert /cert2.txt
```

To confirm that the license certificate has been applied to the provisioned node, use the command `show atmf provision nodes`. The output from this command is shown below, and displays license certification details in the last line.

Figure 19-7: Sample output from the `show atmf provision nodes` command

```
device1#show atmf provision nodes

ATMF Provisioned Node Information:

Backup Media .....: SD (Total 3827.0MB, Free 3481.1MB)

Node Name           : device2
Date & Time         : 06-Oct-2016 & 23:25:44
Provision Path      : card:/atmf/nodes

Boot configuration :
Current boot image  : x510-5.4.6-1.4.rel (file exists)
Backup boot image   : x510-5.4.6-1.3.rel (file exists)
Default boot config : flash:/default.cfg (file exists)
Current boot config : flash:/abc.cfg (file exists)
Backup boot config  : flash:/xyz.cfg (file exists)

Software Licenses :
Repository file     : ../configs/.sw_v2.lic
                   : ../configs/.swfeature.lic
Certificate file    : card:/atmf/lok/nodes/awplus1/flash/.atmf-lic-cert
```

- Related commands**
- [atmf provision \(interface\)](#)
  - [atmf provision node](#)
  - [clone \(amf-provision\)](#)
  - [configure boot config \(amf-provision\)](#)
  - [configure boot system \(amf-provision\)](#)
  - [create \(amf-provision\)](#)
  - [delete \(amf-provision\)](#)
  - [identity \(amf-provision\)](#)
  - [locate \(amf-provision\)](#)
  - [show atmf provision nodes](#)

**Command changes** Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# locate (amf-provision)

**Overview** This command changes the present working directory to the directory of a provisioned node. This makes it easier to edit files and create a unique provisioned node in the backup.

This command can only be run on AMF master nodes.

**NOTE:** We advise that after running this command, you return to a known working directory, typically *flash*.

**Syntax** locate

**Mode** AMF Provisioning

**Example** To change the working directory that happens to be on device1 to the directory of provisioned node device2, use the following command:

```
device1# atmf provision node device2
device1[atmf-provision]# locate
```

The directory of the node device2 should now be the working directory. You can use the command `pwd` to check this, as shown in the following figure.

Figure 19-8: Sample output from the `pwd` command

```
device2#pwd
card:/atmf/building_2/nodes/device2/flash
```

The output above shows that the working directory is now the flash of device2.

**Related commands**

- atmf provision (interface)
- atmf provision node
- clone (amf-provision)
- configure boot config (amf-provision)
- configure boot system (amf-provision)
- copy (amf-provision)
- create (amf-provision)
- delete (amf-provision)
- identity (amf-provision)
- license-cert (amf-provision)
- locate (amf-provision)
- pwd
- show atmf provision nodes



**Command changes** Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# log event-host

**Overview** Use this command to set up an external host to log AMF topology events through Vista Manager. This command is run on the Master device.

Use the **no** variant of this command to disable log events through Vista Manager.

**Syntax** `log event-host [<ipv4-addr>|<ipv6-addr>] atmf-topology-event`  
`no log event-host [<ipv4-addr>|<ipv6-addr>] atmf-topology-event`

| Parameter                      | Description                    |
|--------------------------------|--------------------------------|
| <code>&lt;ipv4-addr&gt;</code> | ipv4 address of the event host |
| <code>&lt;ipv6-addr&gt;</code> | ipv6 address of the event host |

**Default** Log events are disabled by default.

**Mode** Global Configuration

**Usage notes** Event hosts are set so syslog sends the messages out as they come.

Note that there is a difference between log event and log host messages:

- Log event messages are sent out as they come by syslog
- Log host messages are set to wait for a number of messages (20) to send them out together for traffic optimization.

**Example** To enable Node 1 to log event messages from host IP address 192.0.2.31, use the following commands:

```
Node1# configure terminal
```

```
Node1(config)# log event-host 192.0.2.31 atmf-topology-event
```

To disable Node 1 to log event messages from host IP address 192.0.2.31, use the following commands:

```
Node1# configure terminal
```

```
Node1(config)# no log event-host 192.0.2.31 atmf-topology-event
```

**Related commands** [atmf topology-gui enable](#)

# modeltype

**Overview** This command sets the expected model type of the guest node. The model type will default to **other** if nothing is set.

Use the **no** variant of this command to reset the model type to **other**.

**Syntax** `modeltype [alliedware|aw+|onvif|tq|other]`  
`no modeltype`

| Parameter  | Description  |
|------------|--|
| alliedware | A legacy Allied Telesis operating system.                    |
| aw+        | The Allied Telesis AlliedWare Plus operating system.         |
| onvif      | ONVIF (Open Network Video Interface Forum) Profile Q devices |
| tq         | An Allied Telesis TQ Series wireless access point.           |
| other      | Used where the model type is outside the above definitions.  |

**Default** Default to **other**

**Mode** ATMF Guest Configuration Mode

**Example 1** To assign the model type **tq** to the guest-class called 'tq\_device', use the following commands:

```
node1# conf t
node1(config)# atmf guest-class tq_device
node1(config-atmf-guest)# modeltype tq
node1(config-atmf-guest)# end
```

**Example 2** To remove the model type **tq** from the guest-class called 'tq\_device', and reset it to the default of **other**, use the following commands:

```
node1# conf t
node1(config)# atmf guest-class tq_device
node1(config-atmf-guest)# no modeltype
node1(config-atmf-guest)# end
```

**Related commands** [atmf guest-class](#)  
[switchport atmf-guestlink](#)  
[show atmf links guest](#)

**Command changes** Version 5.4.9-2.1: **onvif** parameter added

# service atmf-application-proxy

**Overview** Use this command to enable the AMF Application Proxy service. This service distributes messages across all AMF nodes.

Currently this is used for threat protection. When an AMF Security (AMF-Sec) Controller detects a threat, it issues a request to block the address the threat originated from. The AMF Application Proxy service distributes this message to all AMF nodes. An AMF master accepts this block request and instructs the subordinate AMF node to block the relevant device.

Use the **no** variant of this command to disable the AMF Application Proxy service.

**Syntax** `service atmf-application-proxy`  
`no service atmf-application-proxy`

**Default** The AMF Application Proxy service is disabled by default.

**Mode** Global Configuration

**Usage notes** The AMF master maintains a list of all threats and will send this list to any AMF node, or VCS member, when it boots and joins the AMF network.

In order for this to work the follow must be configured:

- the AMF Application Proxy service on all AMF nodes that need to receive the messages.
- the Hypertext Transfer Protocol (HTTP) service on all nodes that are running the AMF Application Proxy service (see [service http](#)).

**Example** To enable the AMF Application Proxy service, use the commands

```
awplus# configure terminal  
awplus(config)# service atmf-application-proxy
```

To disable the AMF Application Proxy service, use the commands

```
awplus# configure terminal  
awplus(config)# no service atmf-application-proxy
```

**Related commands** [application-proxy threat-protection](#)  
[application-proxy whitelist server](#)  
[clear application-proxy threat-protection](#)  
[show application-proxy threat-protection](#)

**Command changes** Version 5.4.7-2.2: command added

# show application-proxy threat-protection

**Overview** Use this command to list all the IP addresses blocked by the AMF Application Proxy service. It also shows the global threat-detection configuration.

**Syntax** `show application-proxy threat-protection [all]`

| Parameter | Description                               |
|-----------|---|
| all       | Include information for non-local blocks. |

**Mode** Privileged Exec

**Example** To list the addresses blocked by the AMF Application Proxy service, use the command:

```
awplus# show application-proxy threat-protection
```

**Output** Figure 19-9: Example output from **show application-proxy threat-protection**

```
awplus#show application-proxy threat-protection
Quarantine Vlan      : vlan200
Global IP-Filter     : Enabled
IP-Filter Limit Exceeded : 0
Redirect-URL        : http://my.dom/help.html

Client IP           Interface      MAC Address    VLAN    Action
-----
10.34.199.110      -              -              -       link-down
10.34.199.116      port1.0.3     001a.eb93.ec5d 1        drop
10.1.179.1         *              *              *        ip-filter
...
```

Table 19-1: Parameters in the output from **show application-proxy threat-protection**

| Parameter                | Description  |
|--------------------------|--|
| Quarantine Vlan          | The name of the quarantine VLAN.   |
| Global IP-Filter         | The status of global IP filtering.   |
| IP-Filter Limit Exceeded | The number of times an ACL failed to be installed due to insufficient space. |
| Redirect-URL             | The URL a blocked user is redirected to.                                     |

**Related commands** [application-proxy quarantine-vlan](#)  
[application-proxy threat-protection](#)

clear application-proxy threat-protection  
service atmf-application-proxy

**Command changes** Version 5.4.7-2.2: command added

# show application-proxy whitelist interface

**Overview** Use this command to display the status of port authentication on the specified interface.

**Syntax** `show application-proxy whitelist interface [<interface-list>]`

| Parameter                           | Description   |
|-------------------------------------|---|
| <code>&lt;interface-list&gt;</code> | The interfaces or ports to display information about. An interface-list can be: <ul style="list-style-type: none"><li>• a switchport (e.g. port1.0.4)</li><li>• a continuous range of ports separated by a hyphen (e.g. port1.0.1-1.0.4)</li><li>• a comma-separated list (e.g. port1.0.1,port1.0.3-1.0.4). Do not mix port types in the same list.</li></ul> The specified interface must exist. |

**Mode** Privileged Exec

**Example** To display the port authentication information for all interfaces, use the command:

```
awplus# show application-proxy whitelist interface
```

To display the port authentication information for port1.0.4, use the command

```
awplus# show application-proxy whitelist interface port1.0.4
```

**Output** Figure 19-10: Example output from **show application-proxy whitelist interface**

```
awplus#sh application-proxy whitelist interface
Authentication Info for interface port1.0.1
  portEnabled: false - portControl: Auto
  portStatus: Unknown
  reAuthenticate: disabled
  reAuthPeriod: 3600
  PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
  PAE: connectTimeout: 30
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in
  KT: keyTxEnabled: false
  critical: disabled
  guestVlan: disabled
  guestVlanForwarding:
    none
  authFailVlan: disabled
  dynamicVlanCreation: disabled
  multiVlanSession: disabled
  hostMode: single-host
  dot1x: disabled
  authMac: enabled
    method: PAP
    scheme: mac
    reauthRelearning: disabled
  authWeb: disabled
  twoStepAuthentication:
    configured: disabled
    actual: disabled
  supplicantMac: none
  supplicantIpv4: none
Authentication Info for interface port1.0.2
...
```

**Related commands**

- [application-proxy whitelist enable](#)
- [application-proxy whitelist server](#)
- [show application-proxy whitelist server](#)
- [show application-proxy whitelist supplicant](#)

**Command changes** Version 5.4.9-0.1: command added



# show application-proxy whitelist server

**Overview** Use this command to display the external RADIUS server details for the application-proxy whitelist feature.

**Syntax** `show application-proxy whitelist server`

**Mode** Privileged Exec

**Example** To display the external RADIUS server details for the application-proxy whitelist feature, use the command:

```
awplus# show application-proxy whitelist server
```

**Output** Figure 19-11: Example output from **show application-proxy whitelist server**

```
awplus#show application-proxy whitelist server
Application Proxy Whitelist Details:

External Server Details:
  IP: 192.168.1.10
  Port: 1812

Proxy Details:
  IP: 172.31.0.5
  Status: Alive
```

**Related commands**

- [application-proxy whitelist enable](#)
- [application-proxy whitelist server](#)
- [show application-proxy whitelist interface](#)
- [show application-proxy whitelist supplicant](#)

**Command changes** Version 5.4.9-0.1: command added

# show application-proxy whitelist supplicant

**Overview** Use this command to display the current configuration and status for each supplicant attached to an application-proxy whitelist port.

**Syntax** `show application-proxy whitelist supplicant [interface <interface-list> | <mac-addr> | brief]`

| Parameter   | Description   |
|---|---|
| <code>interface</code><br><code>&lt;interface-list&gt;</code> | The interfaces or ports to display information about. An interface-list can be: <ul style="list-style-type: none"><li>• a switchport (e.g. port1.0.4)</li><li>• a continuous range of ports separated by a hyphen (e.g. port1.0.1-1.0.4)</li><li>• a comma-separated list (e.g. port1.0.1,port1.0.3-1.0.4). Do not mix port types in the same list.</li></ul> The specified interface must exist. |
| <code>&lt;mac-addr&gt;</code>                                 | MAC (hardware) address of the supplicant. Entry format is HHHH.HHHH.HHHH (hexadecimal)  |
| <code>brief</code>  | Brief summary of the supplicant state.  |

**Mode** Privileged Exec

**Example** To display the supplicant information for all ports, use the command:

```
awplus# show application-proxy whitelist supplicant
```

To display the supplicant information for port1.0.4, use the command:

```
awplus# show application-proxy whitelist supplicant interface  
port1.0.4
```

**Output** Figure 19-12: Example output from **show application-proxy whitelist supplicant**

```
awplus#show application-proxy whitelist supplicant
Interface port1.0.4
  authenticationMethod: dot1x/mac/web
  Two-Step Authentication
    firstMethod: mac
    secondMethod: dot1x/web
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 0
    webBasedAuthenticationSupplicantNum: 1
    otherAuthenticationSupplicantNum: 0

  Supplicant name: test
  Supplicant address: 001c.233e.e15a
  authenticationMethod: WEB-based Authentication
  Two-Step Authentication:
    firstAuthentication: Pass - Method: mac
    secondAuthentication: Pass - Method: web
  portStatus: Authorized - currentId: 1
  abort:F fail:F start:F timeout:F success:T
  PAE: state: Authenticated - portMode: Auto
  PAE: reAuthCount: 0 - rxRespId: 0
  PAE: quietPeriod: 60 - maxReauthReq: 2
  BE: state: Idle - reqCount: 0 - idFromServer: 0
  CD: adminControlledDirections: in operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
  RADIUS server group (auth): radius
  RADIUS server (auth): 192.168.1.40
  ...
```

**Related commands**

- [application-proxy whitelist enable](#)
- [application-proxy whitelist server](#)
- [show application-proxy whitelist interface](#)
- [show application-proxy whitelist server](#)

**Command changes** Version 5.4.9-0.1: command added

# show atmf

**Overview** Displays information about the current AMF node.

**Syntax** `show atmf [summary|tech|nodes|session]`

| Parameter | Description   |
|-----------|---|
| summary   | Displays summary information about the current AMF node.  |
| tech      | Displays global AMF information.                          |
| nodes     | Displays a list of AMF nodes together with brief details. |
| session   | Displays information on an AMF session.                   |

**Default** Only summary information is displayed.

**Mode** User Exec and Privileged Exec

**Usage notes** AMF uses internal VLANs to communicate between nodes about the state of the AMF network. Two VLANs have been selected specifically for this purpose. Once these have been assigned, they are reserved for AMF and cannot be used for other purposes

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Example 1** To show summary information on AMF node\_1 use the following command:

```
node_1# show atmf summary
```

**Table 20:** Output from the **show atmf summary** command

```
node_1#show atmf summary
ATMF Summary Information:

ATMF Status           : Enabled
Network Name          : Test_network
Node Name              : node_1
Role                   : Master
Restricted login       : Disabled
Current ATMF Nodes    : 3
```

**Example 2** To show information specific to AMF nodes use the following command:

```
node_1# show atmf nodes
```

**Example 3** The **show amf session** command displays all CLI (Command Line Interface) sessions for users that are currently logged in and running a CLI session.

To display AMF active sessions, use the following command:

```
node_1# show atmf session
```

For example, in the output below, node\_1 and node\_5 have active users logged in.

**Table 21:** Output from the **show atmf session** command

```
node_1#show atmf session

CLI Session Neighbors

Session ID           : 73518
Node Name            : node_1
PID                  : 7982
Link type            : Broadcast-cli
MAC Address          : 0000.0000.0000
Options              : 0
Our bits             : 0
Link State           : Full
Domain Controller    : 0
Backup Domain Controller : 0
Database Description Sequence Number : 00000000
First Adjacency      : 1
Number Events        : 0
DBE Retransmit Queue Length : 0
DBE Request List Length : 0
Session ID           : 410804
Node Name            : node_5
PID                  : 17588
Link type            : Broadcast-cli
MAC Address          : 001a.eb56.9020
Options              : 0
Our bits             : 0
Link State           : Full
Domain Controller    : 0
Backup Domain Controller : 0
Database Description Sequence Number : 00000000
First Adjacency      : 1
Number Events        : 0
DBE Retransmit Queue Length : 0
DBE Request List Length : 0
```

**Example 4** The AMF tech command collects all the AMF commands, and displays them. You can use this command when you want to see an overview of the AMF network.

To display AMF technical information, use the following command:

```
node_1# show atmf tech
```

**Table 22:** 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 23:** Parameter definitions from the **show atmf tech** command

| Parameter    | Definition   |
|--------------|--|
| ATMF Status  | The Node's AMF status, either Enabled or Disabled. |
| Network Name | The AMF network that a particular node belongs to. |

**Table 23:** Parameter definitions from the **show atmf tech** command (cont.)

| Parameter          | Definition   |
|--------------------|--|
| Node Name          | The name assigned to a particular node.  |
| Role               | The role configured for this AMF device, either Master or Member.  |
| Current ATMF Nodes | The count of AMF nodes in an AMF Network.  |
| Node Address       | An address used to access a remotely located node (.atmf).   |
| Node ID            | A unique identifier assigned to a Node on an AMF network.  |
| Node Depth         | The number of nodes in path from this node to level of the AMF root node. It can be thought of as the vertical depth of the AMF network from a particular node to the zero level of the AMF root node.   |
| Domain State       | The state of Node in a Domain in AMF network as Controller/Backup.   |
| Recovery State     | The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.   |
| Management VLAN    | The VLAN created for traffic between Nodes of different domain (up/down links). <ul style="list-style-type: none"> <li>• VLAN ID - In this example VLAN 4092 is configured as the Management VLAN.</li> <li>• Management Subnet - Network prefix for the subnet.</li> <li>• Management IP Address - The IP address allocated for this traffic.</li> <li>• Management Mask - The subnet mask used to create a subnet for this traffic (255.255.128.0).</li> </ul> |
| Domain VLAN        | The VLAN assigned for traffic between Nodes of same domain (crosslink). <ul style="list-style-type: none"> <li>• VLAN ID - In this example VLAN 4091 is configured as the domain VLAN.</li> <li>• Domain Subnet. The subnet address used for this traffic.</li> <li>• Domain IP Address. The IP address allocated for this traffic.</li> <li>• Domain Mask. The subnet mask used to create a subnet for this traffic (255.255.128.0).</li> </ul>                 |
| Device Type        | The Product Series name.   |
| ATMF Master        | Whether the node is an AMF master node for its area ('Y' if it is and 'N' if it is not).   |
| SC                 | The device configuration, one of C - Chassis (SBx8100 Series), S - Stackable (VCS) or N - Standalone.  |
| Parent             | The node to which the current node has an active uplink.   |
| Node Depth         | The number of nodes in the path from this node to the master node.   |

**Related commands** [show atmf detail](#)

# show atmf area

**Overview** Use this command to display information about an AMF area. On AMF controllers, this command displays all areas that the controller is aware of. On remote AMF masters, this command displays the controller area and the remote local area. On gateways, this command displays the controller area and remote master area.

**Syntax** `show atmf area [detail] [<area-name>]`

| Parameter   | Description   |
|-------------|---|
| detail      | Displays detailed information   |
| <area-name> | Displays information about master and gateway nodes in the specified area only. |

**Mode** Privileged Exec

**Example 1** To show information about all areas, use the command:

```
controller-1# show atmf area
```

The following figure shows example output from running this command on a controller.

**Table 24:** Example output from the **show atmf area** command on a Controller.

```
controller-1#show atmf area

ATMF Area Information:

* = Local area

Area          Area  Local  Remote  Remote  Node
Name          ID    Gateway Gateway Master   Count
-----
* NZ          1     Reachable  N/A     N/A     3
Wellington   2     Reachable  Reachable  Auth OK  120
Canterbury   3     Reachable  Reachable  Auth Error  -
SiteA-AREA   14    Unreachable  Unreachable  Unreachable  -
Auckland     100   Reachable  Reachable  Auth Start  -
Southland    120   Reachable  Reachable  Auth OK    54

Area count:      6                      Area node count:      177
```

The following figure shows example output from running this command on a remote master.



**Table 25:** Example output from the **show atmf area** command on a remote master.

```

Canterbury#show atmf area

  ATMF Area Information:

  * = Local area

Area          Area  Local      Remote      Remote      Node
Name          ID    Gateway    Gateway     Master      Count
-----
NZ            1     Reachable  N/A         N/A         -
* Canterbury  3     Reachable  N/A         N/A         40

Area count:      2                               Local area node count:  40
    
```

**Table 26:** Parameter definitions from the **show atmf area** command

| Parameter       | Definition  |
|-----------------|---|
| *               | Indicates the area of the device on which the command is being run.   |
| Area Name       | The name of each area.  |
| Area ID         | The ID of the area.   |
| Local Gateway   | Whether the local gateway node is reachable or not.   |
| Remote Gateway  | Whether the remote gateway node is reachable or not. This is one of the following: <ul style="list-style-type: none"> <li>Reachable, if the link has been established.</li> <li>Unreachable, if a link to the remote area has not been established. This could mean that a port or vlan is down, or that inconsistent VLANs have been configured using the <a href="#">switchport atmf-arealink remote-area</a> command.</li> <li>N/A for the area of the controller or remote master on which the command is being run, because the gateway node on that device is local.</li> <li>Auth Start, which may indicate that the area names match on the controller and remote master, but the IDs do not match.</li> <li>Auth Error, which indicates that the areas tried to authenticate but there is a problem. For example, the passwords configured on the controller and remote master may not match, or a password may be missing on the remote master.?</li> <li>Auth OK, which indicates that area authentication was successful and you can now use the <a href="#">atmf select-area</a> command.</li> </ul> |
| Remote Master   | Whether the remote master node is reachable or not. This is N/A for the area of the controller or remote master on which the command is being run, because the master node on that device is local.   |
| Node Count      | The number of nodes in the area.  |
| Area Count      | The number of areas controlled by the controller.   |
| Area Node Count | The total number of nodes in the area.  |

**Example 2** To show detailed information about the areas, use the command:

```
controller-1# show atmf area detail
```

The following figure shows example output from running this command.

**Table 27:** Output from the **show atmf area detail** command

```
controller-1#show atmf area detail

ATMF Area Detail Information:

Controller distance      : 0

Controller Id           : 21
Backup Available        : FALSE

Area Id                 : 2
Gateway Node Name       : controller-1
Gateway Node Id         : 342
Gateway Ifindex         : 6013
Masters Count           : 1
Master Node Name        : well-master (329)
Node Count               : 2

Area Id                 : 3
Gateway Node Name       : controller-1
Gateway Node Id         : 342
Gateway Ifindex         : 4511
Masters Count           : 2
Master Node Name        : cant1-master (15)
Master Node Name        : cant2-master (454)
Node Count               : 2
```

**Related commands**

- [show atmf area summary](#)
- [show atmf area nodes](#)
- [show atmf area nodes-detail](#)

# show atmf area guests

**Overview** This command will display details of all guests that the controller is aware of.

**Syntax** show atmf area guests [*<area-name>*] [*<node-name>*]

| Parameter                | Description                                       |
|--------------------------|---|
| <i>&lt;area-name&gt;</i> | The area name for guest information               |
| <i>&lt;node-name&gt;</i> | The name of the node that connects to the guests. |

**Default** n/a

**Mode** User Exec/Privileged Exec

**Example 1** To display atmf area guest nodes on a controller, use the command,

```
GuestNode[1]#show atmf area guests
```

**Output** Figure 19-13: Example output from the **show atmf area guests** command

```
main-building Area Guest Node Information:
Device      MAC                               IP/IPv6
Type        Address          Parent          Port          Address
-----
-           0008.5d10.7635  x230            1.0.3         192.168.5.4
AT-TQ4600   eccd.6df2.da60  wireless-node1  1.0.4         192.168.5.3
-           0800.239e.f1fe  x230            1.0.4         192.168.4.8
AT-TQ4600   001a.eb3b.dc80  wireless-node2  1.0.7         192.168.4.12

main-building guest node count 4

GuestNode[1]#
```

**Table 28:** Parameters in the output from **show atmf area guests** command

| Parameter   | Description   |
|-------------|---|
| Device Type | The device type as read from the guest node.                        |
| MAC Address | The MAC address of the guest-node                                   |
| Parent      | The device that directly connects to the guest-node                 |
| Port        | The port number on the parent node that connects to the guest node. |
| IP/IPv6     | The IP or IPv6 address of the guest node.                           |

**Related  
commands** [show atmf area](#)  
[show atmf area nodes](#)  
[show atmf backup guest](#)  
[show atmf area guests-detail](#)

# show atmf area guests-detail

**Overview** This command displays the local and remote guest information from an AMF controller.

**Syntax** `show atmf area guests-detail [<area-name> [<node-name>]]`

| Parameter                | Description  |
|--------------------------|--|
| <i>&lt;area-name&gt;</i> | The name assigned to the AMF area. An area is an AMF network that is under the control of an AMF Controller. |
| <i>&lt;node-name&gt;</i> | The name assigned to the network node.   |

**Default** n/a.

**Mode** Privileged Exec

**Example** To display detailed information for all guest nodes attached to “node1”, which is located within the area named “northern”, use the following command:

```
AMF_controller#show atmf area guests-detail northern node1
```

**Output** Figure 19-14: Example output from the **show atmf guest detail** command.

```
#show atmf guest detail

Node Name           : Node1
Port Name           : port1.0.5
Ifindex             : 5005
Guest Description   : tq4600
Device Type         : AT-TQ4600
Configuration Mismatch : No
Backup Supported    : Yes
MAC Address         : ecd.6df2.da60
IP Address          : 192.168.4.50
IPv6 Address        : Not Set
HTTP Port           : 80
Firmware Version    :
Node Name           : poe
Port Name           : port1.0.6
Ifindex             : 5006
Guest Description   : tq3600
Device Type         : AT-TQ2450
Configuration Mismatch : No
Backup Supported    : Yes
MAC Address         : 001a.eb3b.cb80
IP Address          : 192.168.4.9
IPv6 Address        : Not Set
HTTP Port           : 80
Firmware Version    :
```

**Table 29:** Parameters shown in the output of the **show atmf guest detail** command

| Parameter         | Description  |
|-------------------|--|
| Node Name         | The name of the guest's parent node.   |
| Port Name         | The port on the parent node that connects to the guest.  |
| IFindex           | An internal index number that maps to the port number on the parent node.  |
| Guest Description | A brief description of the guest node as manually entered into the <code>description (interface)</code> command for the guest node port on the parent node.                            |
| Device Type       | The device type as supplied by the guest node itself.  |
| Backup Supported  | Indicates whether AMF supports backup of this guest node.  |
| MAC Address       | The MAC address of the guest node.   |
| IP Address        | The IP address of the guest node.  |
| IPv6 Address      | The IPv6 address of the guest node.  |
| HTTP Port         | The HTTP port enables you to specify a port when enabling http to allow a URL for the http user interface of a Guest Node. This is determined by the <code>http-enable</code> command. |
| Firmware Version  | The firmware version that the guest node is currently running.   |

**Related commands** [show atmf area nodes-detail](#)  
[show atmf area guests](#)

# show atmf area nodes

**Overview** Use this command to display summarized information about an AMF controller's remote nodes.

Note that this command can only be run from a controller node.

**Syntax** `show atmf area nodes <area-name> [<node-name>]`

| Parameter   | Description   |
|-------------|---|
| <area-name> | Displays information about nodes in the specified area. |
| <node-name> | Displays information about the specified node.          |

**Mode** Privileged Exec

**Usage notes** If you do not limit the output to a single area or node, this command lists all remote nodes that the controller is aware of. This can be a very large number of nodes.

**Example** To show summarized information for all the nodes in area 'Wellington', use the command:

```
controller-1# show atmf area nodes Wellington
```

The following figure shows partial example output from running this command.

**Table 30:** Output from the **show atmf area nodes Wellington** command

```
controller-1#show atmf area nodes Wellington

Wellington Area Node Information:

Node          Device          ATMF          Node
Name          Type            Master  SC    Parent          Depth
-----
well-gate     x230-18GP       N         N    well-master     1
well-master   AT-x930-28GPX   Y         N    none            0

Wellington node count 2

...
```

**Table 31:** Parameter definitions from the **show atmf area nodes** command

| Parameter   | Definition                              |
|-------------|---|
| Node Name   | The name assigned to a particular node. |
| Device Type | The Product series name.                |

**Table 31:** Parameter definitions from the **show atmf area nodes** command (cont.)

| Parameter   | Definition  |
|-------------|---|
| ATMF Master | Whether the node is an AMF master node for its area ('Y' if it is and 'N' if it is not).              |
| SC          | The device configuration, one of C - Chassis (SBx8100 series), S - Stackable (VCS) or N - Standalone. |
| Parent      | The node to which the current node has an active uplink.  |
| Node Depth  | The number of nodes in the path from this node to the master node.                                    |

**Related commands** [show atmf area](#)  
[show atmf area nodes-detail](#)



# show atmf area nodes-detail

**Overview** Use this command to display detailed information about an AMF controller's remote nodes.

Note that this command can only be run from a controller node.

**Syntax** `show atmf area nodes-detail <area-name> [<node-name>]`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;area-name&gt;</code> | Displays detailed information about nodes in the specified area. |
| <code>&lt;node-name&gt;</code> | Displays detailed information about the specified node.          |

**Mode** Privileged Exec

**Usage notes** If you do not limit the output to a single area or node, this command displays information about all remote nodes that the controller is aware of. This can be a very large number of nodes.

**Example** To show information for all the nodes in area 'Wellington', use the command:

```
controller-1# show atmf area nodes-detail Wellington
```

The following figure shows partial example output from running this command.

**Table 32:** Output from the **show atmf area nodes-detail Wellington** command

```
controller-1#show atmf area nodes-detail Wellington

Wellington Area Node Information:
Node name well-gate
Parent node name : well-master
Domain id       : well-gate's domain
Board type      : 368
Distance to core : 1
Flags           : 50
Extra flags     : 0x00000006
MAC Address     : 001a.eb56.9020

Node name well-master
Parent node name : none
Domain id       : well-master's domain
Board type      : 333
Distance to core : 0
Flags           : 51
Extra flags     : 0x0000000c
MAC Address     : eccd.6d3f.fef7

...
```

**Table 33:** Parameter definitions from the **show atmf area nodes-detail** command

| Parameter        | Definition  |
|------------------|---|
| Node name        | The name assigned to a particular node.   |
| Parent node name | The node to which the current node has an active uplink.                              |
| Domain id        | The name of the domain the node belongs to.   |
| Board type       | The Allied Telesis code number for the device.  |
| Distance to core | The number of nodes in the path from the current node to the master node in its area. |
| Flags            | Internal AMF information  |
| Extra flags      | Internal AMF information  |
| MAC Address      | The MAC address of the current node   |

**Related commands** [show atmf area](#)  
[show atmf area nodes](#)

# show atmf area summary

**Overview** Use this command to display a summary of IPv6 addresses used by AMF, for one or all of the areas controlled by an AMF controller.

**Syntax** `show atmf area summary [<area-name>]`

| Parameter                      | Description                                       |
|--------------------------------|---|
| <code>&lt;area-name&gt;</code> | 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 34:** Output from the **show atmf area summary** command

```
controller-1#show atmf area summary

ATMF Area Summary Information:

Management Information
Local IPv6 Address           : fd00:4154:4d46:1::15

Area Information
Area Name                    : NZ (Local)
Area ID                      : 1
Area Master IPv6 Address     : -

Area Name                    : Wellington
Area ID                      : 2
Area Master IPv6 Address     : fd00:4154:4d46:2::149

Area Name                    : Canterbury
Area ID                      : 3
Area Master IPv6 Address     : fd00:4154:4d46:3::f

Area Name                    : Auckland
Area ID                      : 100
Area Master IPv6 Address     : fd00:4154:4d46:64::17
Interface                    : vlink2000
```

**Related commands**

- [show atmf area](#)
- [show atmf area nodes](#)
- [show atmf area nodes-detail](#)

# show atmf authorization

**Overview** Use this command on an AMF master to display the authorization status of other AMF members and masters on the network.

On an AMF controller this command will show the authorization status of remote area AMF masters.

**Syntax** `show atmf authorization {current|pending|provisional}`

| Parameter   | Description   |
|-------------|---|
| current     | Show the status of all authorized nodes.  |
| pending     | Show the status of unauthorized nodes in the pending queue. These are nodes that enabled secure mode with <code>atmf secure-mode</code> but have not yet been authorized with <code>atmf authorize</code> . |
| provisional | Show the status of provisionally authorized nodes. These are nodes that have been provisioned with <code>atmf authorize provision</code> .  |

**Mode** Privileged Exec

**Example** To display all authorized AMF nodes on an AMF controller or AMF master, use the command:

```
awplus# show atmf authorization current
```

To display AMF nodes which are requesting authorization on an AMF controller or AMF master, use the command:

```
awplus# show atmf authorization pending
```

To display AMF nodes which have provisional authorization, use the command:

```
awplus# show atmf authorization provisional
```

**Output** Figure 19-15: Example output from **show atmf authorization current**

| NZ Authorized Nodes: |          |            |
|----------------------|----------|------------|
| Node Name            | Signer   | Expires    |
| -----                | -----    | -----      |
| master_1             | master_1 | 4 Mar 2017 |
| area_1_node_1        | master_1 | 4 Mar 2017 |
| area_1_node_2        | master_1 | 4 Mar 2017 |

Table 19-1: Parameters in the output from **show atmf authorization current**

| Parameter | Description   |
|-----------|---|
| Node Name | AMF node name of the authorized node.   |
| Signer    | Name of the AMF master that authorized the node.  |
| Expires   | Expiry date of the authorization. Authorization expiry time is set using <code>atmf secure-mode certificate expiry</code> . |

**Output** Figure 19-16: Example output from **show atmf authorization pending**

```

Pending Authorizations:

NZ Requests:
Node Name           Product           Parent Node       Interface
-----
area_1_node_3      x230-18GP        master_1          port1.2.9
area_1_node_4      x510-52GTX       master_1          sal
    
```

Table 19-2: Parameters in the output from **show atmf authorization pending**

| Parameter   | Description  |
|-------------|--|
| Node Name   | Name of the node that is requesting authorization.   |
| Product     | Product name.  |
| Parent Node | Authorization authority of the requesting node.      |
| Interface   | Interface that the authorization request came in on. |

**Output** Figure 19-17: Example output from **show atmf authorization provisional**

```

ATMF Provisional Authorization:

Area - Node Name           Start           Timeout
or MAC Address           Interface       Time           Minutes
-----
3333.4444.5555           5 Sep 2016 02:35:54   3
1111.2222.3333           5 Sep 2016 02:35:24   60
NZ - blue                 port1.0.3       5 Sep 2016 02:35:06   60
    
```

Table 19-3: Parameters in the output from **show atmf authorization provisional**

| Parameter                          | Description  |
|------------------------------------|--|
| Area - Node Name<br>or MAC Address | MAC address or node name of the node that has been provisionally authorized. |
| Interface                          | Interface that the node has been provisioned on.                             |
| Start Time                         | Time the node was provisioned.   |
| Timeout Minutes                    | Length of time from Start Time until the provisional authorization expires.  |

**Related  
commands**

[atmf authorize](#)  
[atmf authorize provision](#)  
[atmf secure-mode](#)  
[clear atmf secure-mode certificates](#)  
[show atmf](#)  
[show atmf secure-mode](#)  
[show atmf secure-mode certificates](#)

**Command  
changes**

Version 5.4.7-0.3: command added

# show atmf backup

**Overview** This command displays information about AMF backup status for all the nodes in an AMF network. It can only be run on AMF master and controller nodes.

**Syntax** show atmf backup  
show atmf backup logs  
show atmf backup server-status  
show atmf backup synchronize [logs]

| Parameter     | Description   |
|---------------|---|
| logs          | Displays detailed log information.  |
| server-status | Displays connectivity diagnostics information for each configured remote file server. |
| synchronize   | Display the file server synchronization status  |
| logs          | For each remote file server, display the logs for the last synchronization            |

**Mode** Privileged Exec

**Example 1** To display the AMF backup information, use the command:

```
node_1# show atmf backup
```

To display log messages to do with backups, use the command:

```
node_1# show atmf backup logs
```

Table 19-4: Output from **show atmf backup**

```
Node_1# show atmf backup
ScheduledBackup .....Enabled
  Schedule.....1 per day starting at 03:00
  Next Backup Time...04 May 2019 03:00
Backup Bandwidth ....Unlimited
Backup Media.....SD (Total 1974.0 MB, Free197.6MB)
Current Action.....Starting manual backup
Started.....04 May 2019 10:08
CurrentNode.....atmf_testbox1
Backup Redundancy ...Enabled
  Local media .....SD (Total 3788.0MB, Free 3679.5MB)
  State .....Active

Node Name          Date           Time           In ATMF  On Media  Status
-----
atmf_testbox1     04 May 2019   09:58:59      Yes      Yes      In Progress
atmf_testbox2     04 May 2019   10:01:23      Yes      Yes      Good
```

Table 19-5: Output from **show atmf backup logs**

```
Node_1#show atmf backup logs

Backup Redundancy ..... Enabled
Local media ..... SD (Total 3788.0MB, Free 1792.8MB)
State ..... Inactive (Remote file server is not available)

Log File Location: card:/atmf/ATMF/logs/rsync_<node name>.log

Node
Name Log Details
-----
atmf_testbox
2019/05/04 18:16:51 [9045] receiving file list
2019/05/04 18:16:51 [9047] .d..t.... flash/
2019/05/04 18:16:52 [9047] >f+++++++ flash/a.rel
```

**Example 2** To display the AMF backup synchronization status, use the command:

```
node_1# show atmf backup synchronize
```

To display log messages to do with synchronization of backups, use the command:

```
node_1# show atmf backup synchronize logs
```

Table 19-6: Output from **show atmf backup synchronize**

```
Node_1#show atmf backup synchronize

ATMF backup synchronization:

* = Active file server

  Id  Date           Time           Status
-----
  1   04 May 2016    22:25:57     Synchronized
* 2   -              -              Active
```

Table 19-7: Output from **show atmf backup synchronize logs**

```
Node_1#show atmf backup synchronize logs

Id    Log Details
-----
1     2019/05/04 22:25:54 [8039] receiving file list
      2019/05/04 22:25:54 [8039] >f..t.... backup_Box1.info
      2019/05/04 22:25:54 [8039] sent 46 bytes received 39 bytes total size 40
```

**Example 3** To display the AMF backup information with the optional parameter **server-status**, use the command:

```
Node_1# show atmf backup server-status
```



```

Node1#sh atmf backup server-status

Id    Last Check    State
-----
1     186 s        File server ready
2     1 s          SSH no route to host
    
```

**Table 20:** Parameter definitions from the **show atmf backup** command

| Parameter         | Definition  |
|-------------------|---|
| Scheduled Backup  | Indicates whether AMF backup scheduling is enabled or disabled.   |
| Schedule          | Displays the configured backup schedule.  |
| Next Backup Time  | Displays the date and time of the next scheduled.   |
| Backup Media      | The current backup medium in use. This will be SD or NONE. SD card only (and not USB) is supported for AMF backup. Utilized and available memory (MB) will be indicated if backup media memory is present.                                  |
| Current Action    | The task that the AMF backup mechanism is currently performing. This will be a combination of either (Idle, Starting, Doing, Stopping), or (manual, scheduled).   |
| Started           | The date and time that the currently executing task was initiated in the format DD MMM YYYY HH:MM   |
| Current Node      | The name of the node that is currently being backed up.   |
| Backup Redundancy | Whether backup redundancy is enabled or disabled.   |
| Local media       | The local media to be used for backup redundancy; SD, USB, INTERNAL, or NONE, and total and free memory available on the media.   |
| State             | Whether SD or USB media is installed and available for backup redundancy. May be Active (if backup redundancy is functional—requires both the local redundant backup media and a remote server to be configured and available) or Inactive. |
| Node Name         | The name of the node that is storing backup data - on its backup media.   |
| Date              | The data of the last backup in the format DD MMM YYYY.  |
| Time              | The time of the last backup in the format HH:MM:SS.   |
| In ATMF           | Whether the node shown is active in the AMF network, (Yes or No).   |
| On Media          | Whether the node shown has a backup on the backup media (Yes or No).  |

**Table 20:** Parameter definitions from the **show atmf backup** command (cont.)

| Parameter         | Definition   |
|-------------------|--|
| Status            | The output can contain one of four values: <ul style="list-style-type: none"><li>• “-” meaning that the status file cannot be found or cannot be read.</li><li>• “Errors” meaning that there are issues - note that the backup may still be deemed successful depending on the errors.</li><li>• “Stopped” meaning that the backup attempt was manually aborted.</li><li>• “Good” meaning that the backup was completed successfully.</li><li>• “In Progress” meaning that the backup is currently running on that node.</li></ul> |
| Log File Location | All backup attempts will generate a result log file in the identified directory based on the node name. In the above example this would be:<br>card:/amf/office/logs/rsync_amf_testbox1.log.   |
| Log Details       | The contents of the backup log file.   |
| server-status     | Displays connectivity diagnostics information for each configured remove file server.  |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Related commands** [show atmf](#)  
[atmf network-name](#)

# show atmf backup area

**Overview** Use this command to display backup status information for the master nodes in one or more areas.

Note that this command is only available on AMF controllers.

**Syntax** `show atmf backup area [<area-name> [<node-name>]] [logs]`

| Parameter   | Description   |
|-------------|---|
| logs        | Displays the logs for the last backup of each node.     |
| <area-name> | Displays information about nodes in the specified area. |
| <node-name> | Displays information about the specified node.          |

**Mode** Privileged Exec

**Example** To show information about backups for an area, use the command:

```
controller-1# show atmf backup area
```

**Table 21:** Output from the **show atmf backup area** command

```

controller-1#show atmf backup area

Scheduled Backup ..... Enabled
  Schedule ..... 12 per day starting at 14:30
  Next Backup Time .... 15 Oct 2016 04:30
Backup Bandwidth ..... Unlimited
Backup Media ..... FILE SERVER 1 (Total 128886.5MB, Free 26234.2MB)
Server Config .....
 * 1 ..... Configured (Mounted, Active)
   Host ..... 10.37.74.1
   Username ..... root
   Path ..... /tftpboot/backups_from_controller-1
   Port ..... -
  2 ..... Configured (Unmounted)
   Host ..... 10.37.142.1
   Username ..... root
   Path ..... -
   Port ..... -
Current Action ..... Idle
  Started ..... -
  Current Node ..... -

Backup Redundancy ..... Enabled
  Local media ..... USB (Total 7604.0MB, Free 7544.0MB)
  State ..... Active

Area Name          Node Name          Id   Date           Time           Status
-----
Wellington         camry              1    14 Oct 2016    02:30:22      Good
Canterbury         corona             1    14 Oct 2016    02:30:23      Good
Canterbury         Avensis           1    14 Oct 2016    02:30:22      Good
Auckland           RAV4              1    14 Oct 2016    02:30:23      Good
Southland          MR2               1    14 Oct 2016    02:30:24      Good
    
```

- Related commands**
- [atmf backup area-masters enable](#)
  - [show atmf area](#)
  - [show atmf area nodes-detail](#)
  - [switchport atmf-arealink remote-area](#)

# show atmf backup guest

**Overview** This command displays backup status information of guest nodes in an AMF network. This command can only be run on a device configured as an AMF Master and has an AMF guest license.

**Syntax** show atmf backup guest [*<node-name>*] [*<guest-port>*] [logs]

| Parameter                 | Description                        |
|---------------------------|------------------------------------|
| <i>&lt;node-name&gt;</i>  | The name of parent guest node      |
| <i>&lt;guest-port&gt;</i> | The port number on the parent node |

**Mode** User Exec/Privileged Exec

**Example** On the switch named x930-master, to display information about the AMF backup guest status, use the command:

```
x930-master# show atmf backup guest
```

**Output** Figure 19-18: Example output from **show atmf backup guest**

```
x930-master#sh atmf backup guest
Guest Backup ..... Enabled
Scheduled Backup ..... Disabled
  Schedule ..... 1 per day starting at 03:00
  Next Backup Time ... 20 Jan 2016 03:00
Backup Bandwidth ..... Unlimited
Backup Media ..... FILE SERVER 2 (Total 655027.5MB,
                          Free 140191.5MB)

Server Config
  1 ..... Configured (Mounted)
  Host ..... 11.0.24.1
  Username ..... bob
  Path ..... guest-project
  Port ..... -
* 2 ..... Configured (Mounted, Active)
  Host ..... 11.0.24.1
  Username ..... bob
  Path ..... guest-project-second
  Port.....-
Current Action .....Idle
Started ..... -
Current Node ..... -
Backup Redundancy ...Enabled
Local media ..... USB (Total 7376.0MB, Free 7264.1MB)
State ..... Active
```

| Parent Node Name | Port Name | Id  | Date        | Time     | Status |
|------------------|-----------|-----|-------------|----------|--------|
| x230             | port1.0.4 | 2   | 19 Jan 2016 | 22:21:46 | Good   |
|                  |           | 1   | 19 Jan 2016 | 22:21:46 | Good   |
|                  |           | USB | 19 Jan 2016 | 22:21:46 | Good   |

Table 19-1: Parameters in the output from **show atmf backup guest**

| Parameter        | Description  |
|------------------|--|
| Guest Backup     | The status of the guest node backup process  |
| Scheduled Backup | The timing configured for guest backups.   |
| Schedule         | Displays the configured backup schedule.   |
| Next Backup Time | The time the next backup process will be initiated.  |
| Backup Bandwidth | The bandwidth limit applied to the backup data flow measured in kilo Bytes /second. Note that unlimited means there is no limit set specifically for the backup data flow. |
| Backup Media     | Detail of the memory media used to store the backup files and the current memory capacity available.   |

- Related commands**
- show atmf backup area
  - show atmf backup
  - show atmf links guest
  - show atmf nodes
  - show atmf backup guest
  - atmf backup guests delete
  - atmf backup guests enable

# show atmf container

**Overview** Use this command to display information about the AMF containers created on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

**Syntax** `show atmf container [detail] [<container-name>]`

| Parameter        | Description  |
|------------------|--|
| detail           | Show detailed information.   |
| <container-name> | The name of the AMF container you wish to display information for. |

**Mode** Privileged Exec

**Output** Figure 19-19: Example output from **show atmf container**

```
awplus#show atmf container
ATMF Container Information:
  Container      Area      Bridge   State    Memory    CPU%
-----
  vac-wlg-1     wlg       br1      running  70.3 MB   1.2
  vac-akl-1     ak1       br2      stopped  0 bytes   0.0
  vac-nsn-1     nsn       br3      running  53.2 MB   0.7
Current ATMF Container count: 3
```

Figure 19-20: Example output from **show atmf container vac-wlg-1**

```
awplus#show atmf container vac-wlg-1
ATMF Container Information:
  Container      Area      Bridge   State    Memory    CPU%
-----
  vac-wlg-1     wlg       br1      running  70.3 MB   1.2
Current ATMF Container count: 1
```

Table 19-2: Parameters in the output from **show atmf container**

| Parameter | Description  |
|-----------|--|
| Container | Name of the AMF container.   |
| Area      | Name of the area the container is in.  |
| Bridge    | Name of the bridge connecting the container to the physical network.   |
| State     | Container state, <code>running</code> or <code>stopped</code> . This is set with the <code>state</code> command. |
| Memory    | The amount of memory the container is using on the VAA host.   |
| CPU%      | The percentage of CPU time the container is using on the VAA, at the time the show command is run.               |

Figure 19-21: Example output from **show atmf container detail vac-wlg-1**

```
awplus#show atmf container detail vac-wlg-1

ATMF Container Information:

Name: vac-wlg-1
State: RUNNING
PID: 980
IP: 172.31.0.1
IP: 192.168.0.2
IP: fd00:4154:4d46:3c::1
CPU use: 3.95 seconds
Memory use: 67.07 MiB
Memory use: 0 bytes
Link: vethP31UFA
TX bytes: 166.01 KiB
RX bytes: 141.44 KiB
Total bytes: 307.45 KiB
Link: vethYCT7BB
TX bytes: 674.27 KiB
RX bytes: 698.27 KiB
Total bytes: 1.34 MiB
```

Table 19-3: Parameters in the output from **show atmf container detail**

| Parameter | Description  |
|-----------|--|
| Name      | Name of the AMF container.   |
| State     | Container state, <code>RUNNING</code> or <code>STOPPED</code> . This is set with the <code>state</code> command. |



Table 19-3: Parameters in the output from **show atmf container detail** (cont.)

| Parameter   | Description  |
|-------------|--|
| PID         | Internal container id.   |
| IP          | This lists the IP addresses used by the container. These include the eth1 IP address and the AMF management IP address.  |
| CPU use     | The CPU usage of the container since it was enabled.   |
| Memory use  | Container memory usage.  |
| Link        | Each container has two links:<br><ol style="list-style-type: none"><li>1 An AMF area-link, this connects the container to the AMF controller and uses virtual interface eth0 on the AMF container.</li><li>2 A bridged L2 network link, this connects the container to the outside world and uses the virtual interface eth1 on the AMF container.</li></ol> See the <a href="#">AMF Feature Overview and Configuration_Guide</a> for more information on these links. |
| TX/RX bytes | Bytes sent and received on a link.   |
| Total bytes | Total bytes transferred on a link.   |

**Related commands**

- area-link
- atmf area
- atmf area password
- atmf container
- atmf container login
- bridge-group
- description (amf-container)
- state

**Command changes**

Version 5.4.7-0.1: command added

# show atmf detail

**Overview** This command displays details about an AMF node. It can only be run on AMF master and controller nodes.

**Syntax** show atmf detail

| Parameter | Description                       |
|-----------|-----------------------------------|
| detail    | Displays output in greater depth. |

**Mode** Privileged Exec

**Example 1** To display the AMF node1 information in detail, use the command:

```
controller-1# show atmf detail
```

A typical output screen from this command is shown below:

```
atmf-1#show atmf detail
ATMF Detail Information:

Network Name           : Test_network
Network Mtu           : 1300
Node Name              : controller-1
Node Address           : controller-1.atmf
Node ID                : 342
Node Depth             : 0
Domain State           : BackupDomainController
Recovery State         : None
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
Domain Subnet          : 172.31.128.0
Domain IP Address     : 172.31.129.86
Domain Mask           : 255.255.128.0
```

**Table 20:** Parameter definitions from the **show atmf detail** command

| Parameter       | Definition   |
|-----------------|--|
| Network MTU     | The network MTU for the ATMF network.  |
| Network Name    | The AMF network that a particular node belongs to.   |
| Node Name       | The name assigned to a particular node.  |
| Node Address    | An Address used to access a remotely located node. This is simply the Node Name plus the dotted suffix atmf (.atmf).   |
| Node ID         | A Unique identifier assigned to a Node on an AMF network.  |
| Node Depth      | The number of nodes in path from this node to level of the AMF root node. It can be thought of as the vertical depth of the AMF network from a particular node to the zero level of the AMF root node.   |
| Domain State    | The state of Node in a Domain in AMF network as Controller/Backup.   |
| Recovery State  | The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.   |
| Management VLAN | The VLAN created for traffic between Nodes of different domain (up/down links). <ul style="list-style-type: none"> <li>• VLAN ID - In this example VLAN 4092 is configured as the Management VLAN.</li> <li>• Management Subnet - Network prefix for the subnet.</li> <li>• Management IP Address - The IP address allocated for this traffic.</li> <li>• Management Mask - The subnet mask used to create a subnet for this traffic (255.255.128.0).</li> </ul> |
| Domain VLAN     | The VLAN assigned for traffic between Nodes of same domain (crosslink). <ul style="list-style-type: none"> <li>• VLAN ID - In this example VLAN 4091 is configured as the domain VLAN.</li> <li>• Domain Subnet. The subnet address used for this traffic.</li> <li>• Domain IP Address. The IP address allocated for this traffic.</li> <li>• Domain Mask. The subnet mask used to create a subnet for this traffic (255.255.128.0).</li> </ul>                 |
| Node Depth      | The number of nodes in the path from this node to the Core domain.   |

# show atmf group

**Overview** This command can be used to display the group membership within to a particular AMF node. It can also be used with the working-set command to display group membership within a working set.

Each node in the AMF is automatically added to the group that is appropriate to its hardware architecture, e.g. x510, x230. Nodes that are configured as masters are automatically assigned to the master group.

You can create arbitrary groups of AMF members based on your own selection criteria. You can then assign commands collectively to any of these groups.

**Syntax** `show atmf group [user-defined|automatic]`

| Parameter                 | Description                             |
|---------------------------|---|
| <code>user-defined</code> | User-defined-group information display. |
| <code>automatic</code>    | Automatic group information display.    |

**Default** All groups are displayed

**Mode** Privileged Exec

**Example 1** To display group membership of node2, use the following command:

```
node2# show atmf group
```

A typical output screen from this command is shown below:

```
ATMF group information

master, x510

node2#
```

This screen shows that node2 contains the groups **master** and **x510**. Note that although the node also contains the implicit groups, these do not appear in the show output.

**Example 2** The following commands (entered on *node2*) will display all the automatic groups within the working set containing *node1* and all nodes that have been pre-defined to contain the *sysadmin* group:

First define the working-set:

```
node1# #atmf working-set node1 group sysadmin
```

A typical output screen from this command is shown below:

```

ATMF group information

master, poe, x8100

=====
node1, node2, node3, node4, node5, node6:
=====

ATMF group information

sysadmin, x8100

AMF_NETWORK[6]#
    
```

This confirms that the six nodes (*node1* to *node6*) are now members of the working-set and that these nodes reside within the *AMF-NETWORK*.

Note that to run this command, you must have previously entered the command [atmf working-set](#) on page 748. This can be seen from the network level prompt, which in this case is *AMF\_NETWORK[6]#*.

**Table 21:** Sample output from the **show atmf group** command for a working set.

```

AMF_NETWORK[6]#show atmf group
=====
node3, node4, node5, node6:
=====

ATMF group information

edge_switches, x510
    
```

**Table 22:** Parameter definitions from the **show atmf group** command for a working set

| Parameter              | Definition  |
|------------------------|---|
| ATMF group information | Displays a list of nodes and the groups that they belong to, for example: <ul style="list-style-type: none"> <li>• master - Shows a common group name for Nodes configured as AMF masters.</li> <li>• Hardware Arch - Shows a group for all Nodes sharing a common Hardware architecture, e.g. x8100, x230, for example.</li> <li>• User-defined - Arbitrary groups created by the user for AMF nodes.</li> </ul> |

# show atmf group members

**Overview** This command will display all group memberships within an AMF working-set. Each node in the AMF working set is automatically added to automatic groups which are defined by hardware architecture, e.g. x510, x230. Nodes that are configured as masters are automatically assigned to the master group. Users can define arbitrary groupings of AMF members based on their own criteria, which can be used to select groups of nodes.

**Syntax** `show atmf group members [user-defined|automatic]`

| Parameter    | Description                            |
|--------------|--|
| user-defined | User defined group membership display. |
| automatic    | Automatic group membership display.    |

**Mode** Privileged Exec

**Example** To display group membership of all nodes in a working-set, use the command:

```
ATMF_NETWORK[9]# show atmf group members
```

**Table 23:** Sample output from the **show atmf group members** command

```
ATMF Group membership
Automatic          Total
Groups            Members  Members
-----
master            1         Building_1
poe               1         HW_Team1
x510              3         SW_Team1 SW_Team2 SW_Team3
x930              1         HW_Team1
x8100             2         Building_1 Building_2

ATMF Group membership
User-defined       Total
Groups            Members  Members
-----
marketing         1         Bld1_Floor_1
software          3         SW_Team1 SW_Team2 SW_Team3
```

**Table 24:** Parameter definitions from the **show atmf group members** command

| Parameter           | Definition   |
|---------------------|--|
| Automatic Groups    | Lists the Automatic Groups and their nodal composition. The sample output shows AMF nodes based on the same Hardware type or belonging to the same Master group. |
| User-defined Groups | Shows the grouping of AMF nodes in user defined groups.  |
| Total Members       | Shows the total number of members in each group.   |
| Members             | Shows the list of AMF nodes in each group.   |

**Related commands**

- [show atmf group](#)
- [show atmf](#)
- [atmf group \(membership\)](#)

# show atmf guests

**Overview** This command is available on any AMF master or controller in the network. It displays a summary of the AMF guest nodes that exist in the AMF network, including device type, parent node, and IP address.

**Syntax** show atmf guests

**Mode** User Exec/Privileged Exec

**Usage notes** Use this command to display all guest nodes in a network. If you want to see only the guests attached to a single node, use the [show atmf links guest](#) command, which shows information about the guest nodes and also about their link to their parent node.

**Example** To display the AMF guest output, use the command:

```
awplus# show atmf guests
```

**Output** Figure 19-22: Example output from the **show atmf guests** command

```
master#show atmf guests

Guest Information:

Device      Device      Parent      Guest      IP/IPv6
Name        Type        Node        Port        Address
-----
node1-2.0.1 x600-24Ts   node1       2.0.1       192.168.2.10
wireless-zone1 AT-TQ4600   node2       1.0.1       192.168.1.10
wireless-zone2 AT-TQ4600   node2       1.0.2       192.168.1.12

Current ATMF guest node count 3
```

**Table 25:** Parameters shown in the output of the **show atmf guests** command

| Parameter   | Description  |
|-------------|--|
| Device Name | The name that is discovered from the device, or failing that, a name that is auto-assigned by AMF. The auto-assigned name consists of: <parent node name>-<attached port number> You can change this by configuring a description on the port.     |
| Device Type | The product name of the guest node, which is discovered from the device. If no device type can be discovered, this shows the name of the AMF guest-class that has been assigned to the guest node by the <a href="#">atmf guest-class</a> command. |



**Table 25:** Parameters shown in the output of the **show atmf guests** command

| Parameter       | Description  |
|-----------------|--|
| Parent Node     | The name of the AMF node that directly connects to the guest node.                                 |
| Guest Port      | The port on the parent node that directly connects to the guest node.                              |
| IP/IPv6 Address | The address discovered from the node, or statically configured on the parent node's attached port. |

**Related  
commands**

[atmf guest-class](#)  
[switchport atmf-guestlink](#)  
[show atmf backup guest](#)  
[show atmf links guest](#)

# show atmf guests detail

**Overview** This command is available on any AMF master in the network. It displays details about the AMF guest nodes that exist in the AMF network, such as device type, IP address, MAC address etc.

**Syntax** `show atmf guests detail [<node-name>] [<guest-port>]`

| Parameter                       | Description                          |
|---------------------------------|--------------------------------------|
| <code>&lt;node-name&gt;</code>  | The name of the guest node's parent. |
| <code>&lt;guest-port&gt;</code> | The port name on the parent node.    |

**Mode** User Exec/Privileged Exec

**Usage notes** If you want to see only the guests attached to a single node, you can use either:

- this command and specify the node name, or
- [show atmf links guest detail](#), which shows information about the guest nodes and also about their link to their parent node.

Note that the parameters that are displayed depend on the guest node's model.

**Example** To display the AMF guest output, use the command:

```
awplus# show atmf guests detail
```

**Output** Figure 19-23: Example output from **show atmf guests detail**

```
master#show atmf guests detail

ATMF Guest Node Information:

Node Name           : master
Port Name           : port1.0.9
Ifindex             : 5009
Guest Description   : red-1.0.9
Device Type         : x600-24Ts
Backup Supported    : No
MAC Address         : 0000.cd38.0c4d
IP Address          : 192.168.1.5
IPv6 Address        : Not Set
HTTP Port           : 0
Firmware Version    : 5.4.2-0.1
```

|                   |                 |
|-------------------|-----------------|
| Node Name         | : node1         |
| Port Name         | : port1.0.13    |
| Ifindex           | : 5013          |
| Guest Description | : node1-1.0.13  |
| Device Type       | : AT-TQ4600     |
| Backup Supported  | : Yes           |
| MAC Address       | : ecd.6df2.daa0 |
| IP Address        | : 192.168.5.6   |
| IPv6 Address      | : Not Set       |
| HTTP Port         | : 80            |
| Firmware Version  | : 3.1.0 B01     |

**Table 26:** Parameters in the output from **show atmf guests detail**.

| Parameter         | Description  |
|-------------------|--|
| Node Name         | The name of the parent node, which is the AMF node that directly connects to the guest node.   |
| Port Name         | The port on the parent node that connects to the guest.  |
| IfIndex           | An internal index number that maps to the port number on the parent node.  |
| Guest Description | A description that is discovered from the device, or failing that, auto-assigned by AMF. The auto-assigned name consists of:<br><parent node name>-<attached port number>.<br>You can change this by configuring a description on the port.        |
| Device Type       | The product name of the guest node, which is discovered from the device. If no device type can be discovered, this shows the name of the AMF guest-class that has been assigned to the guest node by the <a href="#">atmf guest-class</a> command. |
| Username          | The user name configured on the guest node.  |
| Backup Supported  | Whether the guest node supports AMF backup functionality.  |
| MAC Address       | The MAC address of the guest node.   |
| IP Address        | The IP address of the guest node.  |
| IPv6 Address      | The IPv6 address of the guest node.  |
| Firmware Version  | The version of the firmware operating on the guest node.   |
| HTTP port         | The HTTP port as specified with the <a href="#">http-enable</a> command when defining a guest class. You can set this if the guest node provides an HTTP user interface on a non-standard port (any port other than port 80).                      |

**Related  
commands**    `atmf guest-class`  
                  `switchport atmf-guestlink`  
                  `show atmf backup guest`

# show atmf links

**Overview** This command displays information about AMF links on a switch. The display output contains link status state information.

**Syntax** `show atmf links [brief]`

| Parameter | Description   |
|-----------|---|
| brief     | A brief summary of AMF links, their configuration and status. |

**Mode** User Exec and Privileged Exec

**Usage notes** The **show atmf links** and **show atmf links brief** commands both produce a table of summarized link information. For a more detailed view use the [show atmf links detail](#) command.

This command does not show links that are configured on provisioned ports.

**Example** To display a brief summary of the AMF links, use the following command:

```
node-1# show atmf links brief
```

Figure 19-24: Example output from **show atmf links brief**

```
Example-core# show atmf links

ATMF Link Brief Information:

Local      Link      Link      ATMF      Adjacent      Adjacent      Link
Port       Type      Status    State     Node          Ifindex      State
-----
1.0.10     Crosslink Down      Init      *crosslink1  -            Blocking
1.0.14     Crosslink Down      Init      *crosslink2  -            Blocking
1.0.1      Downlink  Down      Init      -            -            Blocking
1.0.2      Downlink  Up        Full      Node2        5001         Forwarding
1.0.8      Downlink  Up        Full      downlink1    5001         Forwarding

* = Provisioned.
```

Table 19-1: Parameter in the output from **show atmf links brief**

| Parameter   | Definition   |
|-------------|--|
| Local Port  | Shows the local port on the selected node.   |
| Link Type   | Shows link type as Uplink or Downlink (parent and child) or Cross-link (nodes in same domain). |
| Link Status | Shows the link status of the local port on the node as either Up or Down.                      |

Table 19-1: Parameter in the output from **show atmf links brief** (cont.)

| Parameter         | Definition  |
|-------------------|---|
| ATMF State        | Shows AMF state of the local port: <ul style="list-style-type: none"> <li>• Init - Link is down.</li> <li>• Hold - Link transitioned to up state, but waiting for hold period to ensure link is stable.</li> <li>• Incompatible - Neighbor rejected the link because of inconsistency in AMF configurations.</li> <li>• OneWay - Link is up and has waited the hold down period and now attempting to link to another unit in another domain.</li> <li>• OneWaySim - Device is running in secure mode and link is up but waiting for authorization from an AMF master.</li> <li>• Full - Link hello packets are sent and received from its neighbor with its own node id.</li> <li>• Shutdown - Link has been shut down by user configuration.</li> </ul> |
| Adjacent Node     | Shows the Adjacent AMF Node to the one being configured.  |
| Adjacent IF Index | Shows the IF index for the Adjacent AMF Node connected to the node being configured.  |
| Link State        | Shows the state of the AMF link. Valid states are either Forwarding or Blocking.  |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare\\_Plus” Feature Overview and Configuration Guide](#).

- Related commands**
- no debug all
  - clear atmf links statistics
  - show atmf
  - show atmf links detail
  - show atmf links guest
  - show atmf links guest detail
  - show atmf links statistics
  - show atmf nodes

# show atmf links detail

**Overview** This command displays detailed information on all the links configured in the AMF network. It can only be run on AMF master and controller nodes.

**Syntax** `show atmf links detail`

| Parameter | Description                     |
|-----------|---------------------------------|
| detail    | Detailed AMF links information. |

**Mode** User Exec

**Usage notes** For summarized link information see the [show atmf links](#) command.  
This command does not show links that are configured on provisioned ports.

**Example** To display the AMF link details use this command:

```
device1# show atmf links detail
```

The output from this command will display all the internal data held for AMF links. The following example gives details of the links that are summarized in the example in [show atmf links](#).

**Table 20:** Sample output from the **show atmf links detail** command

```
device1# show atmf links detail
-----
Crosslink Ports Information
-----
Port                : sa1
Ifindex             : 4501
Port Status         : Down
Port State          : Init
Last event          :
Port BPDU Receive Count : 0
Port                : po10
Ifindex             : 4610
Port Status         : Up
Port State          : Full
Last event          : AdjNodeLSEPresent
Port BPDU Receive Count : 140
Adjacent Node Name  : Building-B
Adjacent Ifindex    : 4610
Adjacent MAC        : eccd.6ddl.64d0
Port Last Message Response : 0
```

**Table 20:** Sample output from the **show atmf links detail** command (cont.)

```
Port : po30
Ifindex : 4630
Port Status : Up
Port State : Full
Last event : AdjNodeLSEPresent
Port BPDU Receive Count : 132
Adjacent Node Name : Building-A
Adjacent Ifindex : 4630
Adjacent MAC : eccd.6daa.c861
Port Last Message Response : 0

Link State Entries:

Crosslink Ports Blocking : False
Node.Ifindex : Building-A.4630 - Example-core.4630
Transaction ID : 2 - 2
MAC Address : eccd.6daa.c861 - 0000.cd37.054b
Link State : Full - Full

Node.Ifindex : Building-B.4610 - Example-core.4610
Transaction ID : 2 - 2
MAC Address : eccd.6ddl.64d0 - 0000.cd37.054b
Link State : Full - Full

Domain Nodes Tree:

Node : Building-A
  Links on Node : 1
  Link 0 : Building-A.4630 - Example-core.4630
  Forwarding State : Forwarding
Node : Building-B
  Links on Node : 1
  Link 0 : Building-B.4610 - Example-core.4610
  Forwarding State : Forwarding
Node : Example-core
  Links on Node : 2
  Link 0 : Building-A.4630 - Example-core.4630
  Forwarding State : Forwarding
  Link 1 : Building-B.4610 - Example-core.4610
  Forwarding State : Forwarding

Crosslink Transaction Entries:

Node : Building-B
Transaction ID : 2
Uplink Transaction ID : 6
Node : Building-A
Transaction ID : 2
Uplink Transaction ID : 6

Uplink Information:

Waiting for Sync : 0
Transaction ID : 6
Number of Links : 0
Number of Local Uplinks : 0
```



**Table 20:** Sample output from the **show atmf links detail** command (cont.)

```
Originating Node      : Building-A
Domain                : -'s domain
Node                  : Building-A
Ifindex               : 0
Node Depth            : 0
Transaction ID        : 6
Flags                 : 32
Domain Controller     : -
Domain Controller MAC : 0000.0000.0000

Originating Node      : Building-B
Domain                : -'s domain
Node                  : Building-B
Ifindex               : 0
Node Depth            : 0
Transaction ID        : 6
Flags                 : 32
Domain Controller     : -
Domain Controller MAC : 0000.0000.0000

Downlink Domain Information:

Domain                : Dept-A's domain
  Domain Controller    : Dept-A
  Domain Controller MAC : eccd.6d20.c1d9
  Number of Links      : 2
  Number of Links Up   : 2
  Number of Links on This Node : 2
  Links are Blocked    : 0
  Node Transaction List
    Node               : Building-B
    Transaction ID     : 8
    Node               : Building-A
    Transaction ID     : 8
  Domain List
    Domain             : Dept-A's domain
    Node               : Example-core
    Ifindex            : 4621
    Transaction ID     : 8
    Flags              : 1
    Domain             : Dept-A's domain
    Node               : Example-core
    Ifindex            : 4622
    Transaction ID     : 8
    Flags              : 1
```

**Table 20:** Sample output from the **show atmf links detail** command (cont.)

```
Domain : Dorm-D's domain
Domain Controller : Dorm-D
Domain Controller MAC : 0000.cd37.082c
Number of Links : 2
Number of Links Up : 2
Number of Links on This Node : 2
Links are Blocked : 0
Node Transaction List
Node : Building-B
Transaction ID : 20
Node : Building-A
Transaction ID : 20
Domain List
Domain : Dorm-D's domain
Node : Building-A
Ifindex : 0
Transaction ID : 20
Flags : 32
Domain : Dorm-D's domain
Node : Building-B
Ifindex : 0
Transaction ID : 20
Flags : 32
Domain : Dorm-D's domain
Node : Example-core
Ifindex : 4510
Transaction ID : 20
Flags : 1
Domain : Dorm-D's domain
Node : Example-core
Ifindex : 4520
Transaction ID : 20
Flags : 1
Domain : Example-edge's domain
Domain Controller : Example-edge
Domain Controller MAC : 001a.eb93.7aa6
Number of Links : 1
Number of Links Up : 1
Number of Links on This Node : 0
Links are Blocked : 0
Node Transaction List
Node : Building-B
Transaction ID : 9
Node : Building-A
Transaction ID : 9
```

**Table 20:** Sample output from the **show atmf links detail** command (cont.)

```
Domain List
Domain          : Example-edge's domain
Node            : Building-A
Ifindex         : 0
Transaction ID  : 9
Flags           : 32
Domain          : Example-edge's domain
Node            : Building-B
Ifindex         : 5027
Transaction ID  : 9
Flags           : 1
-----
Up/Downlink Ports Information
-----
Port            : sa10
Ifindex         : 4510
Port Status     : Up
Port State      : Full
Last event      : LinkComplete
Adjacent Node   : Dorm-A
Adjacent Internal ID : 211
Adjacent Ifindex : 4510
Adjacent Board ID : 387
Adjacent MAC    : eccd.6ddf.6cdf
Adjacent Domain Controller : Dorm-D
Adjacent Domain Controller MAC : 0000.cd37.082c
Port Forwarding State : Forwarding
Port BPDU Receive Count : 95
Port Sequence Number : 11
Port Adjacent Sequence Number : 7
Port Last Message Response : 0
Port            : po21
Ifindex         : 4621
Port Status     : Up
Port State      : Full
Last event      : LinkComplete
Adjacent Node   : Dept-A
Adjacent Internal ID : 29
Adjacent Ifindex : 4621
Adjacent Board ID : 340
Adjacent MAC    : eccd.6d20.c1d9
Adjacent Domain Controller : Dept-A
Adjacent Domain Controller MAC : eccd.6d20.c1d9
Port Forwarding State : Forwarding
Port BPDU Receive Count : 96
Port Sequence Number : 8
Port Adjacent Sequence Number : 9
Port Last Message Response : 0
Special Link Present : FALSE
```

**Table 21:** Parameter definitions from the **show atmf links detail** command output

| Parameter                     | Definition   |
|-------------------------------|--|
| Crosslink Ports Information   | <p>Show details of all Crosslink ports on this Node:</p> <ul style="list-style-type: none"> <li>• Port - Name of the Port or static aggregation (sa&lt;*&gt;).</li> <li>• Ifindex - Interface index for the crosslink port.</li> <li>• VR ID - Virtual router id for the crosslink port.</li> <li>• Port Status - Status of the local port on the Node as UP or DOWN.</li> <li>• Port State - AMF State of the local port.                             <ul style="list-style-type: none"> <li>– Init - Link is down.</li> <li>– Hold - Link transitioned to up state, but waiting for hold period to ensure link is stable.</li> <li>– Incompatible - Neighbor rejected the link because of inconsistency in AMF configurations.</li> <li>– OneWay - Link is up and has waited the hold down period and now attempting to link to another unit in another domain</li> <li>– Full - Link hello packets are sent and received from its neighbor with its own node id.</li> <li>– Shutdown - Link has been shut down by user configuration.</li> </ul> </li> </ul> <p>Port BPDU Receive Count - The number of AMF protocol PDU's received.</p> <ul style="list-style-type: none"> <li>• Adjacent Node Name - The name of the adjacent node connected to this node.</li> <li>• Adjacent Ifindex - Adjacent AMF Node connected to this Node.</li> <li>• Adjacent VR ID - Virtual router id of the adjacent node in the domain.</li> <li>• Adjacent MAC - MAC address of the adjacent node in the domain.</li> <li>• Port Last Message Response - Response from the remote neighbor to our AMF last hello packet.</li> </ul> |
| Link State Entries            | <p>Shows all the link state database entries:</p> <ul style="list-style-type: none"> <li>• Node.Ifindex - Shows adjacent Node names and Interface index.</li> <li>• Transaction ID - Shows transaction id of the current crosslink transaction.</li> <li>• MAC Address - Shows adjacent Node MAC addresses.</li> <li>• Link State - Shows AMF states of adjacent nodes on the link.</li> </ul>   |
| Domain Nodes Tree             | <p>Shows all the nodes in the domain:</p> <ul style="list-style-type: none"> <li>• Node - Name of the node in the domain.</li> <li>• Links on Node - Number of crosslinks on a vertex/node.</li> <li>• Link no - Shows adjacent Node names and Interface index.</li> <li>• Forwarding State - Shows state of AMF link Forwarding/Blocking.</li> </ul>  |
| Crosslink Transaction Entries | <p>Shows all the transaction entries:</p> <ul style="list-style-type: none"> <li>• Node - Name of the AMF node.</li> <li>• Transaction ID - transaction id of the node.</li> <li>• Uplink Transaction ID - transaction id of the remote node.</li> </ul>   |

**Table 21:** Parameter definitions from the **show atmf links detail** command output (cont.)

| Parameter                   | Definition  |
|-----------------------------|---|
| Uplink Information          | <p>Show all uplink entries.</p> <ul style="list-style-type: none"> <li>• Waiting for Sync - Flag if uplinks are currently waiting for synchronization.</li> <li>• Transaction ID - Shows transaction id of the local node.</li> <li>• Number of Links - Number of up downlinks in the domain.</li> <li>• Number of Local Uplinks - Number of uplinks on this node to the parent domain.</li> <li>• Originating Node - Node originating the uplink information.</li> <li>• Domain - Name of the parent uplink domain.</li> <li>• Node - Name of the node in the parent domain, that is connected to the current domain.</li> <li>• Ifindex - Interface index of the parent node's link to the current domain.</li> <li>• VR ID - Virtual router id of the parent node's link to the current domain.</li> <li>• Transaction ID - Transaction identifier for the neighbor in crosslink.</li> <li>• Flags - Used in domain messages to exchange the state:<br/>           ATMF_DOMAIN_FLAG_DOWN = 0<br/>           ATMF_DOMAIN_FLAG_UP = 1<br/>           ATMF_DOMAIN_FLAG_BLOCK = 2<br/>           ATMF_DOMAIN_FLAG_NOT_PRESENT = 4<br/>           ATMF_DOMAIN_FLAG_NO_NODE = 8<br/>           ATMF_DOMAIN_FLAG_NOT_ACTIVE_PARENT = 16<br/>           ATMF_DOMAIN_FLAG_NOT_LINKS = 32<br/>           ATMF_DOMAIN_FLAG_NO_CONFIG = 64</li> <li>• Domain Controller - Domain Controller in the uplink domain</li> <li>• Domain Controller MAC - MAC address of Domain Controller in uplink domain</li> </ul> |
| Downlink Domain Information | <p>Shows all the downlink entries:</p> <ul style="list-style-type: none"> <li>• Domain - Name of the downlink domain.</li> <li>• Domain Controller - Controller of the downlink domain.</li> <li>• Domain Controller MAC - MAC address of the domain controller.</li> <li>• Number of Links - Total number of links to this domain from the Node.</li> <li>• Number of Links Up - Total number of links that are in UP state.</li> <li>• Number of Links on This Node - Number of links terminating on this node.</li> <li>• Links are Blocked - 0 links are not blocked to the domain. 1 All links are blocked to the domain.</li> </ul>   |

**Table 21:** Parameter definitions from the **show atmf links detail** command output (cont.)

| Parameter                     | Definition  |
|-------------------------------|---|
| Node Transaction List         | <p>List of transactions from this downlink domain node.</p> <ul style="list-style-type: none"> <li>• Node - 0 links are not blocked to the domain. 1 All links are blocked to the domain.</li> <li>• Transaction ID - Transaction id for this node.</li> <li>• Domain List: Shows list of nodes in the current domain and their links to the downlink domain.:</li> <li>• Domain - Domain name of the downlink node.</li> <li>• Node - Name of the node in the current domain.</li> <li>• Ifindex - Interface index for the link from the node to the downlink domain.</li> <li>• Transaction ID - Transaction id of the node in the current domain.</li> <li>• Flags - As mentioned above.</li> </ul>  |
| Up/Downlink Ports Information | <p>Shows all the configured up and down link ports on this node:</p> <ul style="list-style-type: none"> <li>• Port - Name of the local port.</li> <li>• Ifindex - Interface index of the local port.</li> <li>• VR ID - Virtual router id for the local port.</li> <li>• Port Status - Shows status of the local port on the Node as UP/DOWN.</li> <li>• Port State - AMF state of the local port.</li> <li>• Adjacent Node - nodename of the adjacent node.</li> <li>• Adjacent Internal ID - Unique node identifier of the remote node.</li> <li>• Adjacent Ifindex - Interface index for the port of adjacent AMF node.</li> <li>• Adjacent Board ID - Product identifier for the adjacent node.</li> <li>• Adjacent VR ID - Virtual router id for the port on adjacent AMF node.</li> <li>• Adjacent MAC - MAC address for the port on adjacent AMF node.</li> <li>• Adjacent Domain Controller - nodename of the Domain controller for Adjacent AMF node.</li> <li>• Adjacent Domain Controller MAC - MAC address of the Domain controller for Adjacent AMF node.</li> <li>• Port Forwarding State - Local port forwarding state Forwarding or Blocking.</li> <li>• Port BPDU Receive Count - count of AMF protocol PDU's received.</li> <li>• Port Sequence Number - hello sequence number, incremented every time the data in the hello packet changes.</li> <li>• Port Adjacent Sequence Number - remote ends sequence number used to check if we need to process this packet or just note it arrived.</li> <li>• Port Last Message Response - response from the remote neighbor to our last hello packet.</li> </ul> |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Related commands** no debug all  
clear atmf links statistics  
show atmf

# show atmf links guest

**Overview** This command displays information about guest nodes visible to an AMF device.

**Syntax** show atmf links guest [interface <interface-range>]

| Parameter                      | Description  |
|--------------------------------|--|
| interface<br><interface-range> | Select a specific range of ports to display information about guest nodes. |

**Default** With no parameters specified this command will display its standard output for all ports with guest nodes connected.

**Mode** User Exec/Privileged Exec

**Usage notes** Use this command to display the guest nodes connected to a single parent node. If you want to see a list of all the guests in the AMF network, use [show atmf guests](#).

**Example 1** To display information about AMF guests that are connectible from node1, use the command:

```
node1# show atmf links guest
```

**Output** Figure 19-25: Example output from **show atmf links guest**

```
node1#sh atmf links guest

Guest Link Information:

DC = Discovery configuration
   S = static D = dynamic

Local   Guest      Model      MAC      IP / IPv6
Port    Class       Type       DC Address Address
-----
1.0.1   -           other      D 0013.1a1e.4589 192.168.1.2
1.0.2   aastra-phone other      D 0008.5d10.7635 192.168.1.3
1.0.3   cisco-phone2 other      S -              192.168.2.1
1.0.4   panasonic... other      D 0800.239e.f1fe 192.168.1.5
```

Table 19-1: Parameters in the output from **show atmf links guest**

| Parameter   | Description  |
|-------------|--|
| Local Port  | The port on the parent node that connects to the guest.  |
| Guest Class | The name of the ATMF guest-class that has been assigned to the guest node by the <a href="#">atmf guest-class</a> command. |



Table 19-1: Parameters in the output from **show atmf links guest** (cont.)

| Parameter         | Description  |
|-------------------|--|
| Model Type        | The model type of the guest node, as entered by the <code>modeltype</code> command. Can be one of the following: <ul style="list-style-type: none"><li>• alliedware</li><li>• aw+</li><li>• tq</li><li>• other</li></ul> |
| DC                | The discovery method as applied by the <code>discovery</code> command. This can be either dynamic (D) or static (S).   |
| MAC Address       | The MAC address of the guest node.   |
| IP / IPv6 Address | The IP address of the guest node.  |

**Related commands**

- `atmf guest-class`
- `discovery`
- `http-enable`
- `username`
- `modeltype`
- `switchport atmf-guestlink`
- `show atmf backup guest`

# show atmf links guest detail

**Overview** This command displays detailed information about guest nodes visible to an AMF device.

**Syntax** `show atmf links guest detail [interface <interface-range>]`

| Parameter                      | Description  |
|--------------------------------|--|
| interface<br><interface-range> | Select a specific range of ports to display information about guest nodes. |

**Mode** User Exec/Privileged Exec

**Usage notes** Use this command to display the guest nodes connected to a single parent node. If you want to see a list of all the guests in the AMF network, use [show atmf guests detail](#).

Note that the parameters that are displayed depend on the guest node's model and state.

**Example** To display detailed information about AMF guests, use the command:

```
node1# show atmf links guest detail
```

**Output** Figure 19-26: Example output from **show atmf links guest detail**

```
node1#show atmf links guest detail

Detailed Guest Link Information:

Interface : port1.0.13
Link State : Down
Class Name : test
Model Type : Other
Discovery Method : Static
IP Address : 192.168.1.13
Node State : Down

Interface : port1.0.17
Link State : Full
Class Name : access
Model Type : TQ
Discovery Method : Dynamic
IP Address : 192.168.5.8
Username : manager
Node State : Full
Backup Supported : Yes
MAC address : 001a.ebad.ce60
Device Type : AT-TQ3400
Description : node1-1.0.17
Firmware Version : 3.2.1 A02
```

Table 19-2: Parameters in the output from **show atmf links guest detail**

| Parameter        | Description   |
|------------------|---|
| Interface        | The port on the parent node that connects to the guest.   |
| Link State       | The state of the link to the guest node; one of: <ul style="list-style-type: none"> <li>• Down: The physical link is down.</li> <li>• Up: The physical link has come up, but it is still during a timeout period that is enforced to allow other links to come up.</li> <li>• Learn: The timeout period described above has elapsed, and the link is now learning information from the AMF guest node. You can see what information it is learning from the "Node State" field below.</li> <li>• Full: The node connected by this link has joined the AMF network.</li> <li>• Fail: The port is physically up but something has prevented the guest node from joining the AMF network.</li> </ul> |
| Class Name       | The name of the ATMF guest-class that has been assigned to the guest node by the <code>atmf guest-class</code> command.   |
| Model Type       | The model type of the guest node, as entered by the <code>modeltype</code> command. Can be one of the following: <ul style="list-style-type: none"> <li>• alliedware</li> <li>• aw+</li> <li>• onvif</li> <li>• tq</li> <li>• other</li> </ul>  |
| Discovery Method | The discovery method as applied by the <code>discovery</code> command. This can be either dynamic or static.  |
| IP Address       | The IP address of the guest node.   |
| Username         | The user name configured on the guest node.   |

Table 19-2: Parameters in the output from **show atmf links guest detail** (cont.)

| Parameter        | Description   |
|------------------|---|
| Node state       | The state of the guest node; one of: <ul style="list-style-type: none"> <li>• Down: The initial state when a link to a guest node is first configured. This is also the state if the physical link goes down.</li> <li>• Getting IP: The AMF device is in the process of retrieving the IP address of the guest node.</li> <li>• Getting Mac: The AMF device is in the process of retrieving the MAC address of the guest node.</li> <li>• Getting Info: The AMF device is in the process of retrieving any other available information from the guest (firmware version etc). The information available depends on what device the guest node is.</li> <li>• Full: The AMF device has retrieved all necessary information and the guest node has joined the AMF network. Once this state is reached, the Link State also changes to "Full".</li> <li>• Failure: The physical link is up but the AMF member has failed to retrieve enough information to allow the guest node to join the AMF network.</li> </ul> |
| Backup Supported | Whether the guest node supports AMF backup functionality.   |
| MAC Address      | The MAC address of the guest node.  |
| Device Type      | Model information for the guest node. This field shows the model information that AMF retrieved from the guest node. In contrast, the Model Type shows what a user entered as the type of device they intended this guest node to be.   |
| Description      | By default, this is a concatenation of the guest node's parent node and the port to which it is attached. You can change it by configuring a description on the port.   |
| Serial Number    | The serial number of the guest node.  |
| Firmware Name    | The name of the firmware operating on the guest node.   |
| Firmware Version | The version of the firmware operating on the guest node.  |
| HTTP port        | The HTTP port as specified with the <a href="#">http-enable</a> command when defining a guest class. You can set this if the guest node provides an HTTP user interface on a non-standard port (any port other than port 80).   |

**Related commands**

- [atmf guest-class](#)
- [discovery](#)
- [http-enable](#)

username  
modeltype  
switchport atmf-guestlink  
show atmf backup guest

# show atmf links statistics

**Overview** This command displays details of the AMF links configured on the device and also displays statistics about the AMF packet exchanges between the devices.

It is also possible to display the AMF link configuration and packet exchange statistics for a specified interface.

This command can only be run on AMF master and controller nodes

**Syntax** `show atmf links statistics [interface [<port-number>]]`

| Parameter     | Description  |
|---------------|--|
| interface     | Specifies that the command applies to a specific interface (port) or range of ports. Where both the interface and port number are unspecified, full statistics (not just those relating to ports) will be displayed.     |
| <port-number> | Enter the port number for which statistics are required. A port range, a static channel or LACP link can also be specified. Where no port number is specified, statistics will be displayed for all ports on the device. |

**Mode** User Exec

**Example 1** To display AMF link statistics for the whole device, use the command:

```
device1# show atmf links statistics
```

**Table 20:** Sample output from the **show atmf links statistics** command

| ATMF Statistics:       |         |          |
|------------------------|---------|----------|
|                        | Receive | Transmit |
| -----                  |         |          |
| Arealink Hello         | 318     | 327      |
| Crosslink Hello        | 164     | 167      |
| Crosslink Hello Domain | 89      | 92       |
| Crosslink Hello Uplink | 86      | 88       |
| Hello Link             | 0       | 0        |
| Hello Neighbor         | 628     | 630      |
| Hello Stack            | 0       | 0        |
| Hello Gateway          | 1257    | 1257     |
| Database Description   | 28      | 28       |
| Database Request       | 8       | 6        |
| Database Update        | 66      | 162      |
| Database Update Bitmap | 0       | 29       |
| Database Acknowledge   | 144     | 51       |

**Table 20:** Sample output from the **show atmf links statistics** command (cont.)

```

Transmit Fails          0          1
Discards                0          0
Total ATMF Packets     2788      2837

ATMF Database Statistics:

Database Entries        18
Database Full Ages      0
ATMF Virtual Link Statistics:

Virtual                Receive      Receive      Transmit      Transmit
link                  Receive      Dropped      Transmit      Dropped
-----
vlink2000             393         0            417          0

ATMF Packet Discards:
Type0  0      : Gateway hello msg received from unexpected neighbor
Type1  0      : Stack hello msg received from unexpected neighbor
Type2  0      : Discard TX update bitmap packet - bad checksum
Type3  0      : Discard TX update packet - neighbor not in correct state
Type4  0      : Discard update packet - bad checksum or type
Type5  0      : Discard update packet - neighbor not in correct state
Type6  0      : Discard update bitmap packet - bad checksum or type
Type7  0      : Incarnation is not possible with the data received
Type8  0      : Discard crosslink hello received - not correct state
Type9  0      : Discard crosslink domain hello received on non crosslink
Type10 0      : Discard crosslink domain hello - not in correct state
Type11 0      : Crosslink uplink hello received on non crosslink port
Type12 0      : Discard crosslink uplink hello - not in correct state
Type13 0      : Wrong network-name for this ATMF
Type14 0      : Packet received on port is too long
Type15 0      : Bad protocol version, received on port
Type16 0      : Bad packet checksum calculation
Type17 0      : Bad authentication type
Type18 0      : Bad simple password
Type19 0      : Unsupported authentication type
Type20 0      : Discard packet - unknown neighbor
Type21 0      : Discard packet - port is shutdown
Type22 0      : Non broadcast hello msg received from unexpected neighbor
Type23 0      : Arealink hello msg received on non arealink port
Type24 0      : Discard arealink hello packet - not in correct state
Type25 0      : Discard arealink hello packet - failed basic processing
Type26 0      : Discard unicast packet - MAC address does not match node
Type27 0      : AMF Master license node limit exceeded
    
```

**Example 2** To display the AMF links statistics on interface port1.0.4, use the command:

```
device1# show atmf links statistics interface port1.0.4
```

Figure 19-27: Sample output from the **show atmf links statistics** command for interface port1.0.4

```

device1# show atmf links statistics interface port1.0.4

ATMF Port Statistics:

-----
port1.0.4  Crosslink Hello                231      232
port1.0.4  Crosslink Hello Domain          116      116
port1.0.4  Crosslink Hello Uplink          116      115
port1.0.4  Hello Link                       0         0
port1.0.4  Arealink Hello                   0         0
    
```

Figure 19-28: Parameter definitions from the **show atmf links statistics** command output

| Parameter            | Definition   |
|----------------------|--|
| Receive              | Shows a count of AMF protocol packets received per message type.       |
| Transmit             | Shows the number of AMF protocol packets transmitted per message type. |
| Database Entries     | Shows the number of AMF elements existing in the distributed database. |
| Database Full Ages   | Shows the number of times the entries aged in the database.            |
| ATMF Packet Discards | Shows the number of discarded packets of each type.                    |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

- Related commands**
- no debug all
  - clear atmf links statistics
  - show atmf



# show atmf nodes

**Overview** This command displays nodes currently configured within the AMF network.

Note that the output also tells you whether or not node map exchange is active. Node map exchange improves the tracking of nodes joining and leaving an AMF network. This improves the efficiency of AMF networks. Node map exchange is only available if every node in your AMF network is running version 5.4.6-2.1 or later. We recommend running the latest version on all nodes in your network, so you receive the advantages of node map exchange and other improvements.

**Syntax** `show atmf nodes [guest|all]`

| Parameter | Description  |
|-----------|--|
| guest     | Display only guest nodes in the AMF network.                 |
| all       | Display all nodes in the AMF network, including guest nodes. |

**Mode** Privileged Exec

**Usage notes** You can use this command to display one of three sets of nodes:

- all nodes except guest nodes, by specifying **show atmf nodes**
- all nodes including guest nodes, by specifying **show atmf nodes all**
- only guest nodes, by specifying **show atmf nodes guest**

**Examples** To display AMF information for all nodes except guest nodes, use the command:

```
node1# show atmf nodes
```

Table 19-1: Sample output from **show atmf nodes**

```
node1#show atmf nodes guest

Node Information:

* = Local device

SC = Switch Configuration:
C = Chassis   S = Stackable   N = Standalone

Node          Device          ATMF          Parent          Node
Name          Type            Master SC          Domain          Depth
-----
* M1          x510-28GTX      Y             S              none           0
N3           x230-18GP       N             N              M1             1
N1           AR4050S         N             N              M1             1

Node map exchange is active
Current ATMF node count 3
```

To display AMF information for all nodes, including guest nodes, use the command:

```
node1# show atmf nodes all
```

**Table 20:** Sample output from **show atmf nodes all**. In this example, not all nodes support node map exchange, as shown by the message at the end

```
node1#show atmf nodes all

Node and Guest Information:

* = Local device

SC = Switch Configuration:
C = Chassis  S = Stackable  N = Standalone G = Guest

Node/Guest      Device          ATMF          Parent          Node
Name           Type            Master SC   Domain          Depth
-----
* M1            x510-28GTX     Y      S   none           0
N3              x230-18GP     N      N   M1             1
N1              AR4050S       N      N   M1             1
N3-1.0.24      AT-TQ4600     N      G   N3             -

Node map exchange is inactive
Firmware on some nodes does not support node map exchange, eg AR4050S
Current ATMF node count 4 (guests 1)
```

To display AMF information for guest nodes only, use the command:

```
node1# show atmf nodes guest
```

**Table 19-1:** Sample output from **show atmf nodes guest**

```
node1#show atmf nodes guest

Guest Information:
Device      MAC
Name        Address      Parent          Port          IP/IPv6
Address
-----
aastra-...  0008.5d10.7635 Node-1          1.0.2         192.168.4.7
poe-1.0.1   0013.1a1e.4589 Node-1          1.0.1         192.168.4.6
ip-camera   0800.239e.f1fe Node-1          1.0.4         192.168.4.8
tq4600      eccd.6df2.da60 Node-1          1.0.5         192.168.4.50
```

- Related commands**
- [show atmf](#)
  - [show atmf area nodes](#)
  - [discovery](#)
  - [http-enable](#)
  - [show atmf backup guest](#)

# show atmf provision nodes

**Overview** This command displays information about each provisioned node with details about date and time of creation, boot and configuration files available in the backup, and license files present in the provisioned backup. This includes nodes that have joined the network but are yet to run their first backup.

This command can only be run on AMF master and controller nodes.

**Syntax** `show atmf provision nodes`

**Mode** Privileged Exec

**Usage notes** This command will only work if provisioned nodes have already been set up. Otherwise, an error message is shown when the command is run.

**Example** To show the details of all the provisioned nodes in the backup use the command:

```
NodeName# show atmf provision nodes
```

Figure 19-29: Sample output from the **show atmf provision nodes** command

```
device1#show atmf provision nodes

ATMF Provisioned Node Information:

Backup Media .....: SD (Total 3827.0MB, Free 3481.1MB)

Node Name           : device2
Date& Time          : 06-Oct-2016 & 23:25:44
Provision Path      : card:/atmf/provision_nodes

Boot configuration :
Current boot image  : x510-5.4.9-0.1.rel (file exists)
Backup boot image   : x510-5.4.8-2.3.rel (file exists)
Default boot config : flash:/default.cfg (file exists)
Current boot config : flash:/abc.cfg (file exists)
Backup boot config  : flash:/xyz.cfg (file exists)

Software Licenses :
Repository file     : ../configs/.sw_v2.lic
                   : ../configs/.swfeature.lic
Certificate file    : card:/atmf/nodes/awplus1/flash/.atmf-lic-cert
```

- Related commands**
- [atmf provision \(interface\)](#)
  - [atmf provision node](#)
  - [clone \(amf-provision\)](#)
  - [configure boot config \(amf-provision\)](#)
  - [configure boot system \(amf-provision\)](#)
  - [create \(amf-provision\)](#)

delete (amf-provision)  
identity (amf-provision)  
license-cert (amf-provision)  
locate (amf-provision)

# show atmf recovery-file

**Overview** Use this command to display the recovery file information for an AMF node. AMF recovery files are created for nodes with special links. Special links include:

- virtual links,
- area links terminating on an AMF master, and
- area virtual links terminating on an AMF master.

**Syntax** `show atmf recovery-file`

**Mode** Privileged Exec

**Example** To display recovery file information for an AMF node, use the command:

```
node1# show atmf recovery-file
```

**Output** Figure 19-30: Example output from **show atmf recovery-file**

```
node1#show atmf recovery-file

ATMF Recovery File Info: Special Link Present
Location                Date           Time
USB storage device      30 Apr 2018   14:50:32
Master                  30 Apr 2018   14:56:45
node1                   30 Apr 2018   14:56:45
node3                   30 Apr 2018   14:56:45
```

**Related commands** [clear atmf recovery-file](#)  
[show atmf backup](#)

**Command changes** Version 5.4.8-0.2: command added

# show atmf secure-mode

**Overview** Use this command to display an overview of the secure mode status of an AMF network.

**Syntax** show atmf secure-mode

**Mode** Privileged Exec

**Example** To display an overview of AMF secure mode on an AMF master or member node, use the command:

```
awplus# show atmf secure-mode
```

**Output** Figure 19-31: Example output from **show atmf secure-mode** on an AMF master

```
ATMF Secure Mode:

Secure Mode Status           : Enabled
Certificate Expiry           : 180 Days
Certificates Total            : 8
Certificates Revoked          : 0
Certificates Rejected         : 0
Certificates Active          : 8

Provisional Authorization    : 0
Pending Requests             : 0

Trusted Master                : master_1
Trusted Master                : master_2

Key Fingerprint:
 48:37:d9:a0:37:32:22:9b:5c:22:da:a2:62:49:a7:e5:a9:bc:12:88
```

Figure 19-32: Example output from **show atmf secure-mode** on an AMF node

```
ATMF Secure Mode:

Secure Mode Status           : Enabled
Trusted Master                : master_1
Trusted Master                : master_2

Key Fingerprint:
 93:f0:52:a9:74:8f:ae:ea:5b:e2:ee:62:cb:6b:21:22:5a:08:db:98
```

Table 19-2: Parameters in the output from **show atmf secure-mode**

| Parameter                 | Description  |
|---------------------------|--|
| Secure Mode Status        | Shows the status of secure mode, Enabled or Disabled.  |
| Certificate Expiry        | Certificate expiry time. Set with <a href="#">atmf secure-mode certificate expiry</a>  |
| Certificates Total        | Total number of certificates.  |
| Certificates Revoked      | Certificates that have been revoked by the AMF master.   |
| Certificates Rejected     | Certificates that have been rejected by the AMF master.  |
| Certificates Active       | Certificates that are currently active.  |
| Provisional Authorization | Number of nodes with provisional authorization. For more information use the <a href="#">show atmf authorization provisional</a> command.          |
| Pending Requests          | Number of nodes waiting for authorization on the AMF master. For more information use the <a href="#">show atmf authorization pending</a> command. |
| Trusted Master            | List of trusted masters in the AMF area.   |
| Key Fingerprint           | The AMF node's key fingerprint.  |

**Related commands**

- [atmf authorize](#)
- [atmf secure-mode](#)
- [atmf secure-mode certificate expiry](#)
- [show atmf authorization](#)
- [show atmf secure-mode audit link](#)

**Command changes**

- Version 5.4.7-0.3: command added

# show atmf secure-mode audit

**Overview** Use this command to detect security vulnerabilities on a node.

**Syntax** show atmf secure-mode audit

**Mode** Privileged Exec

**Example** To display AMF secure mode link audits for a node, use the command  
awplus# show atmf secure-mode audit

**Output** Figure 19-33: Example output from **show atmf secure-mode audit**

```
ATMF Secure Mode Audit:

Warning   : The default username and password is enabled.
Good      : SNMP V1 or V2 is disabled.
Warning   : Telnet server is enabled.
Good      : ATMF is enabled. Secure-Mode is on.
Good      : ATMF Topology-GUI is disabled. No trustpoints configured.

ATMF Secure Mode Log Events:

-----
2017 Feb 2 00:59:25 user.notice node1 ATMF[848]: Sec_Audit - ATMF Secure
Mode is enabled.
2017 Feb 2 01:30:00 user.notice node1 ATMF[848]: Sec_Audit - Established
secure connection to area_1_node_1 on interface vlink1.
```

Table 19-3: Parameters in the output from **show atmf secure-mode audit link**

| Parameter                   | Description   |
|-----------------------------|---|
| ATMF Secure Mode Audit      | A list of security recommendations to secure the AMF network. Items prefaced with <code>Warning</code> need to be fixed. In the sample above the default username and password, and telnet, should be disabled. |
| ATMF Secure Mode Log Events | A list of recorded secure mode log events.  |

**Related commands** [show atmf secure-mode](#)

**Command changes** Version 5.4.7-0.3: command added



# show atmf secure-mode audit link

**Overview** Use this command to detect security vulnerabilities by identifying devices that are connected to a secure mode node that are not in secure mode or are not authorized.

**Syntax** `show atmf secure-mode audit link`

**Mode** Privileged Exec

**Example** To display AMF secure mode link audits for a node, use the command  
`awplus# show atmf secure-mode audit link`

**Output** Figure 19-34: Example output from **show atmf secure-mode audit link**

```
ATMF Secure Mode Audit Link:

* ATMF links connected to devices which are not authorized
  or are not in secure-mode.

Port          Link Type   Discovered          Node/Area Name
-----
vlink1       Downlink   16/02/2017 09:28:22 Member3
```

Table 19-4: Parameters in the output from **show atmf secure-mode audit link**

| Parameter      | Description                         |
|----------------|-------------------------------------|
| Port           | Port name on local device.          |
| Link Type      | Link type.                          |
| Discovered     | Date discovered                     |
| Node/Area Name | Node or area name of remote device. |

**Related commands** [show atmf](#)  
[show atmf secure-mode](#)

**Command changes** Version 5.4.7-0.3: command added

# show atmf secure-mode certificates

**Overview** Use this command to display the certificate status details when secure mode is enabled on an AMF network.

**Syntax** `show atmf secure-mode certificates [detail] [area <area-name>] [node <node-name>]`

| Parameter   | Description   |
|-------------|---|
| detail      | Display detailed certificate information.                     |
| area        | Specify an AMF area.  |
| <area-name> | The AMF area you want to see the certificate information for. |
| node        | Specify an AMF node.  |
| <node-name> | The AMF node you want to see information for.                 |

**Mode** Privileged Exec

**Example** To display AMF secure mode certificates on a master or member node, use the command:

```
awplus# show atmf secure-mode certificates
```

To display detailed information about AMF secure mode certificates for a node named "area\_2\_node\_1" in an area named "area-2", use the command:

```
awplus# show atmf secure-mode certificates detail area area-2 node area_2_node_1
```

**Output** Figure 19-35: Example output from **show atmf secure-mode certificates**

```
Area-1 Certificates:
Node Name          Signer             Expires            Status
-----
area_1_node_1     master_1           11 Mar 2017
area_1_node_1     master_2           4 Mar 2017        Active
area_1_node_2     master_1           11 Mar 2017
area_1_node_2     master_2           4 Mar 2017        Revoked

Area-2 Certificates:
Node Name          Signer             Expires            Status
-----
area_2_node_1     master_1           18 Mar 2017        Active
area_2_node_2     master_1           18 Mar 2017        Rejected
```

Table 19-5: Parameters in the output from **show atmf secure-mode certificates**

| Parameter | Description   |
|-----------|---|
| Node Name | Name of AMF node the certificate was issued to.   |
| Signer    | Name of AMF master that issued the certificate.   |
| Expires   | Certificate expiry date.  |
| Status    | The status column will display <i>Active</i> before a member node is trusted, and can be accessed using AMF commands. Valid statuses are <i>Active</i> , <i>Revoked</i> , and <i>Rejected</i> . |

**Output** Figure 19-36: Example output from **show atmf secure-mode certificates detail area area-2 node area\_2\_node\_1**

```
Certificates Detail:
-----
area_2_node_1 (area:area-2)
  MAC Address      : 0000.cd37.0003
  Status           : Active
  Serial Number    : A24SC8001
  Product          : x510-28GTX
  Key Fingerprint  : cd:b4:c9:cd:7b:87:6a:30:98:25:d7:3c:89:8e:cb:74:e8:91:56:9d
  Flags            : 00000011
  Signer           : master_1
  Expiry Date      : 18 Mar 2017 21:17:42
```

Table 19-6: Parameters in the output from **show atmf secure-mode certificates detail**

| Parameter       | Description  |
|-----------------|--|
| MAC Address     | MAC address of AMF node.   |
| Status          | The device status will show <i>Active</i> if a member node is trusted, and can be accessed using AMF commands. Valid statuses are <i>Active</i> , <i>Revoked</i> , and <i>Rejected</i> . |
| Serial Number   | Device serial number.  |
| Product         | Device product type.   |
| Key Fingerprint | AMF node key fingerprint.  |
| Flags           | Internal AMF information.  |
| Signer          | Name of AMF master that issued the certificate.  |
| Expiry Date     | Certificate expiry date.   |

**Related commands**

- atmf authorize
- atmf secure-mode
- atmf secure-mode certificate expire
- atmf secure-mode certificate renew
- clear atmf secure-mode certificates
- show atmf secure-mode sa

**Command changes** Version 5.4.7-0.3: command added

# show atmf secure-mode sa

**Overview** Use this command to display the security associations on the network. This is the list of links and neighbors that are trusted.

**Syntax** `show atmf secure-mode sa [detail] [link|neighbor|broadcast]`

| Parameter | Description  |
|-----------|--|
| detail    | Display detailed security association information. |
| link      | Display security associations for type links.      |
| neighbor  | Display security associations for type neighbors.  |
| broadcast | Display security associations for type broadcast.  |

**Mode** Privileged Exec

**Example** To display an overview of AMF secure mode security associations on a master or member node, use the command:

```
awplus# show atmf secure-mode sa
```

To display a detailed overview of AMF secure mode neighbor security associations on a master or member node, use the command:

```
awplus# show atmf secure-mode sa detail neighbor
```

**Output** Figure 19-37: Example output from **show atmf secure-mode sa**

```
ATMF Security Associations:
```

| Type                 | State         | ID       | Details    |
|----------------------|---------------|----------|------------|
| Neighbor Node        | Complete      | 175      | master_1   |
| Broadcast            | Complete      | 4095     |            |
| CrossLink            | Complete      | 4501     | sa1        |
| AreaLink             | Cert Exchg    | 4511     | sa11       |
| Link                 | Complete      | 6009     | port1.2.9  |
| AreaLink             | CA Exchg Init | 6013     | port1.2.13 |
| AreaLink             | Cert Exchg    | 13001    | port1.9.1  |
| Link                 | CA Exchg Init | 16779521 | vlink3     |
| Neighbor Gateway     | Complete      | 83       | master_2   |
| Neighbor Gateway     | Complete      | 175      | master_1   |
| Neighbor Cntl-Master | Complete      | 83       | master_2   |
| Neighbor Cntl-Master | Complete      | 175      | master_1   |

Figure 19-38: Example output from **show atmf secure-mode sa detail neighbor**

```
Security Associations Detail:
-----
Id           : 175 (af)
  Type       : Neighbor Node
  State      : Complete
  Remote MAC Address : eccd.6d82.6c16
  Flags      : 000003c0

Id           : 83 (40000053)
  Type       : Neighbor Gateway
  State      : Complete
  Remote MAC Address : 001a.eb54.e53b
  Flags      : 000003c0

Id           : 175 (400000af)
  Type       : Neighbor Gateway
  State      : Complete
  Remote MAC Address : eccd.6d82.6c16
  Flags      : 000003c0

Id           : 83 (80000053)
  Type       : Neighbor Cntl-Master
  State      : Complete
  Remote MAC Address : 001a.eb54.e53b
  Flags      : 000003c0

Id           : 175 (800000af)
  Type       : Neighbor Cntl-Master
  State      : Complete
  Remote MAC Address : eccd.6d82.6c16
  Flags      : 000003c0

Id           : 321 (80000141)
  Type       : Neighbor Cntl-Master
  State      : Complete
  Remote MAC Address : 0000.f427.93da
  Flags      : 000003c0
```

Table 19-7: Parameters in the output from **show atmf secure-mode sa**

| Parameter          | Description   |
|--------------------|---|
| Type               | Security Association (SA) types: <ul style="list-style-type: none"> <li>• Link - SA for link</li> <li>• CrossLink - SA for crosslink</li> <li>• AreaLink - SA for area link</li> <li>• Neighbor Node - SA for node neighbor relationship</li> <li>• Neighbor Gateway - SA for gateway neighbor relationship</li> <li>• Neighbor Cntl-Master - SA for controller/master neighbor relationship</li> <li>• Broadcast - SA for working-set broadcast requests</li> </ul>                                  |
| State              | Current state of the Security Association. The state must be Complete before a member node is trusted, and can be accessed using AMF commands. <ul style="list-style-type: none"> <li>• CA Exchg Init - SA is ready to begin the SA exchange process</li> <li>• CA Exchg - SA is currently exchanging CAs</li> <li>• Cert Exchg - SA is currently exchanging certificates</li> <li>• Key Exchg - SA is currently exchanging ephemeral keys</li> <li>• Complete - SA exchange has completed</li> </ul> |
| ID                 | Security Association ID. <ul style="list-style-type: none"> <li>• For Neighbor types this is the remote node ID.</li> <li>• For Link types this is the local ifindex.</li> <li>• For Broadcast type this is always 4095.</li> </ul>   |
| Details            | Human readable translation of ID. <ul style="list-style-type: none"> <li>• For Neighbor types this is the node name</li> <li>• For Link types this is the interface name</li> </ul>   |
| Remote MAC Address | MAC address of the remote partner of the security association.  |
| Flags              | Internal AMF information.   |

**Related commands** [atmf secure-mode](#)  
[show atmf secure-mode](#)  
[show atmf secure-mode certificates](#)

**Command changes** Version 5.4.7-0.3: command added

# show atmf secure-mode statistics

**Overview** Use this command to display AMF secure mode statistics. These statistics are from when AMF secure mode was first enabled or the statistics were cleared with the `clear atmf secure-mode statistics` command.

**Syntax** `show atmf secure-mode statistics`

**Mode** Privileged Exec

**Example** To display AMF secure mode statistics on a master or member node, use the command:

```
awplus# show atmf secure-mode statistics
```

**Output** Figure 19-39: Example output from `show atmf secure-mode statistics` on an AMF master.

```
ATMF Secure Mode Statistics:

Certificates:
New ..... 7                Expired ..... 0
Updated ..... 7            Deleted ..... 0
Revoked ..... 1           Renewed ..... 2
Rejected ..... 1          Re-authorized .... 1
Authorized ..... 0

Local Certificates:
Valid ..... 4                Invalid ..... 0
Certificates Validation:
Request Valid ..... 2
Request Invalid ..... 0
Common Valid ..... 13
Common Invalid ..... 0
Issuer Valid ..... 14
Issuer Invalid ..... 0
Signature Verified ..... 29
Signature Invalid ..... 0
Signature Purpose Invalid ..... 0

Signatures Signed ..... 12
Master Certificates:
Re-issued ..... 3
Downgraded to member ..... 0

Public key change ..... 2
Invalid SA public key ..... 0
```



**Output** Figure 19-40: Example output from **show atmf secure-mode statistics** on an AMF node.

```
ATMF Secure Mode Statistics:

Local Certificates:
Valid ..... 3          Invalid ..... 0

Certificates Validation:
Request Valid ..... 0
Request Invalid ..... 0
Common Valid ..... 0
Common Invalid ..... 0
Issuer Valid ..... 12
Issuer Invalid ..... 0
Signature Verified ..... 12
Signature Invalid ..... 3
Signature Purpose Invalid ..... 0

Signatures Signed ..... 0

Master Certificates:
Re-issued ..... 0
Downgraded to member ..... 0

Public key change ..... 2
Invalid SA public key ..... 0
```

- Related commands**
- [atmf authorize](#)
  - [atmf secure-mode](#)
  - [atmf secure-mode certificate renew](#)
  - [clear atmf secure-mode statistics](#)
  - [show atmf secure-mode](#)

**Command changes** Version 5.4.7-0.3: command added

# show atmf tech

**Overview** This command collects and displays all the AMF command output. The command can thus be used to display a complete picture of an AMF network.

**Syntax** show atmf tech

**Mode** Privileged Exec

**Example** To display output for all AMF commands, use the command:

```
NodeName# show atmf tech
```

**Table 20:** Sample output from the **show atmf tech** command.

```
node1#show atmf tech
ATMF Summary Information:

ATMF Status           : Enabled
Network Name          : ATMF_NET
Node Name              : node1
Role                   : Master
Current ATMF Nodes    : 8

ATMF Technical information:

Network Name           : ATMF_NET
Domain                 : node1's domain
Node Depth             : 0
Domain Flags           : 0
Authentication Type    : 0
MAC Address            : 0014.2299.137d
Board ID               : 287
Domain State           : DomainController
Domain Controller      : node1
Backup Domain Controller : node2
Domain controller MAC  : 0014.2299.137d
Parent Domain          : -
Parent Domain Controller : -
Parent Domain Controller MAC : 0000.0000.0000
Number of Domain Events : 0
Crosslink Ports Blocking : 0
Uplink Ports Waiting on Sync : 0
```

**Table 20:** Sample output from the **show atmf tech** command. (cont.)

|                                   |         |
|-----------------------------------|---------|
| Crosslink Sequence Number         | : 7     |
| Domains Sequence Number           | : 28    |
| Uplink Sequence Number            | : 2     |
| Number of Crosslink Ports         | : 1     |
| Number of Domain Nodes            | : 2     |
| Number of Neighbors               | : 5     |
| Number of Non Broadcast Neighbors | : 3     |
| Number of Link State Entries      | : 1     |
| Number of Up Uplinks              | : 0     |
| Number of Up Uplinks on This Node | : 0     |
| DBE Checksum                      | : 84fc6 |
| Number of DBE Entries             | : 0     |
| ...                               |         |

**Table 21:** Parameter definitions from the **show atmf tech** command

| Parameter          | Definition   |
|--------------------|--|
| ATMF Status        | Shows status of AMF feature on the Node as Enabled/Disabled.   |
| Network Name       | The name of the AMF network to which this node belongs.  |
| Node Name          | The name assigned to the node within the AMF network.  |
| Role               | The role configured on the device within the AMF - either master or member.  |
| Current ATMF Nodes | A count of the AMF nodes in the AMF network.   |
| Node Address       | The identity of a node (in the format name.atmf) that enables its access it from a remote location.  |
| Node ID            | A unique identifier assigned to an AMF node.   |
| Node Depth         | The number of nodes in the path from this node to the core domain.   |
| Domain State       | A node's state within an AMF Domain - either controller or backup.   |
| Recovery State     | The AMF node recovery status. Indicates whether a node recovery is in progress on this device - either Auto, Manual, or None.  |
| Management VLAN    | The VLAN created for traffic between nodes of different domains (up/down links).<br>VLAN ID - In this example VLAN 4092 is configured as the Management VLAN.<br>Management Subnet - the Network prefix for the subnet.<br>Management IP Address - the IP address allocated for this traffic.<br>Management Mask - the Netmask used to create a subnet for this traffic 255.255.128.0 (= prefix /17) |

**Table 21:** Parameter definitions from the **show atmf tech** command (cont.)

| Parameter   | Definition  |
|-------------|---|
| Domain VLAN | The VLAN assigned for traffic between Nodes of same domain (crosslink).<br>VLAN ID - In this example VLAN 4091 is configured as the domain VLAN.<br>Domain Subnet - the Subnet address used for this traffic.<br>Domain IP Address - the IP address allocated for this traffic.<br>Domain Mask - the Netmask used to create a subnet for this traffic 255.255.128.0<br>(= prefix /17) |
| Device Type | Shows the Product Series Name.  |
| ATMF Master | Indicates the node's membership of the core domain (membership is indicated by Y)   |
| SC          | Shows switch configuration: <ul style="list-style-type: none"><li>• C - Chassis (such as SBx8100 series)</li><li>• S - Stackable (VCS)</li><li>• N - Standalone</li></ul>   |
| Parent      | A node that is connected to the present node's uplink, i.e. one layer higher in the hierarchy.  |
| Node Depth  | Shows the number of nodes in path from the current node to the Core domain.   |

**NOTE:** The **show atmf tech** command can produce very large output. For this reason only the most significant terms are defined in this table.

# show atmf virtual-links

**Overview** This command displays a summary of all virtual links (L2TP tunnels) currently in the running configuration.

**Syntax** `show atmf virtual-links [macaddr]`

| Parameter | Description                                   |
|-----------|---|
| macaddr   | Display the virtual AMF links' MAC addresses. |

**Mode** Privileged Exec

**Example 1** To display AMF virtual links, use the command:

```
node_1# show atmf virtual-links
```

Table 19-1: Example output from **show atmf virtual-links**

```
ATMF Link Remote Information:

Local      Local      Remote      Tunnel      Tunnel
Port      ID   IP          ID   IP          Protect     State
-----
vlink1    1    172.16.24.2  2    1.0.0.2     -           Complete
vlink2    2    172.16.24.2* 10   172.16.24.3* ipsec       Complete
vlink3    3    (eth0)*      1    1.2.3.4     -           AcquireLocal

* = Dynamic Address.

Virtual Links Configured: 3
```

In the above example, a centrally located switch has the IP address space 192.0.2.x/24. It has two VLANs assigned the subnets 192.0.2.33 and 192.0.2.65 using the prefix /27. Each subnet connects to a virtual link. The first link has the IP address 192.168.1.1 and has a Local ID of 1. The second has the IP address 192.168.2.1 and has the Local ID of 2.

**Example 2** To display AMF virtual links' MAC address information, use the command:

```
node_1# show atmf virtual-links macaddr
```

Table 19-2: Example output from **show atmf virtual-links macaddr**

```

ATMF Link Remote Information:

ATMF Management Bridge Information:

Bridge: br-atmfmgmt

port no mac addr                is local?    ageing timer
  1      00:00:cd:27:c2:07        yes          0.00
  2      8e:c7:ae:81:7e:68        yes          0.00
  2      00:00:cd:28:bf:e7        no           0.01
    
```

Table 19-3: Parameters in the output from **show atmf virtual-links**

| Parameter    | Definition   |
|--------------|--|
| vlink1       | The tunnel named vlink1, equivalent to an L2TP tunnel.   |
| Local ID     | The local ID of the virtual link. This matches the vlink<number>   |
| State        | The operational state of the vlink (either Up or Down). This state is always displayed once a vlink has been created.                      |
| mac addr     | AMF virtual links terminate on an internal soft bridge. The “show atmf virtual-links macaddress” command displays MAC Address information. |
| is local?    | Indicates whether the MAC displayed is for a local or a remote device.   |
| ageing timer | Indicates the current aging state for each MAC address.  |

**Related commands** [atmf virtual-link](#)

# show atmf working-set

**Overview** This command displays the nodes that form the current AMF working-set.

**Syntax** show atmf working-set

**Mode** Privileged Exec

**Example** To show current members of the working-set, use the command:

```
ATMF_NETWORK[6]# show atmf working-set
```

**Table 20:** Sample output from the **show atmf working-set** command.

```
ATMF Working Set Nodes:
node1, node2, node3, node4, node5, node6
Working set contains 6 nodes
```

**Related commands**

- [atmf working-set](#)
- [show atmf](#)
- [show atmf group](#)

# show debugging atmf

**Overview** Use this command to see what debugging is turned on for AMF.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show debugging atmf`

**Mode** Privileged Exec

**Example** To display the AMF debugging status, use the command:

```
node_1# show debugging atmf
```

Table 19-1: Sample output from the **show debugging atmf** command.

```
node_1# show debugging atmf
ATMF debugging status:
ATMF arealink debugging is on
ATMF link debugging is on
ATMF crosslink debugging is on
ATMF database debugging is on
ATMF neighbor debugging is on
ATMF packet debugging is on
ATMF error debugging is on
```

**Related commands** [debug atmf packet](#)



# show debugging atmf packet

**Overview** Use this command to see what debugging is turned on for AMF Packet debug. For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show debugging atmf packet`

**Mode** User Exec and Privileged Exec

**Example** To display the AMF packet debugging status, use the command:

```
node_1# show debug atmf packet
```

Table 19-2: Sample output from the **show debugging atmf packet** command.

```
ATMF packet debugging is on
=== ATMF Packet Debugging Parameters===
Node Name: x908
Port name: port1.1.1
Limit: 500 packets
Direction: TX
Info Level: Level 2
Packet Type Bitmap:
2. Crosslink Hello BPDU pkt with downlink domain info
3. Crosslink Hello BPDU pkt with uplink info
4. Down and up link Hello BPDU pkts
6. Stack hello unicast pkts
8. DBE request
9. DBE update
10. DBE bitmap update
```

**Related commands** [debug atmf](#)  
[debug atmf packet](#)

# show running-config atmf

**Overview** This command displays the running system information that is specific to AMF.

**Syntax** `show running-config atmf`

**Mode** User Exec and Global Configuration

**Example** To display the current configuration of AMF, use the following commands:

```
node_1# show running-config atmf
```

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Related commands** `show running-config`  
`no debug all`

# state

**Overview** This command sets the running state of an AMF container on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

**Syntax** `state {enable|disable}`

| Parameter | Description  |
|-----------|--|
| disable   | Stop the AMF container. The container's state changes to stopped.  |
| enable    | Start the AMF container. The container's state changes to running. |

**Default** By default, **state** is disabled.

**Mode** AMF Container Configuration

**Usage notes** The first time the **state enable** command is executed on a container it assigns the container to an area and configures it as an AMF master. This is achieved by automatically adding the following configuration to the AMF container:

```
atmf network-name <AMF network-name>
atmf master
atmf area <container area-name> <container area-id> local
atmf area <container area-name> password <container area-password>
atmf area <host area-name> <host area-id>

interface eth0
  atmf-arealink remote-area <host area-name> vlan 4094
```

For this reason the **state enable** command should be run after the container has been created with the [atmf container](#) command and an area-link configured with the [area-link](#) command.

Once the start-up configuration has been saved from within the AMF container, all further configuration changes need to be made manually.

**Example** To start the AMF container “vac-wlg-1” use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# state enable
```

To stop the AMF container “vac-wlg-1” use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# state disable
```

**Related commands** [atmf container](#)  
[show atmf container](#)

**Command changes** Version 5.4.7-0.1: command added

# switchport atmf-agentlink

**Overview** Use this command to configure a link between this device and an x600 Series switch, in order to integrate the x600 Series switch into your AMF network. The x600 Series switch is called an “AMF agent”, and the link between the x600 and this device is called an “agent link”.

The x600 Series switch must be running version 5.4.2-3.16 or later.

Use the **no** variant of this command to remove the agent link. If the x600 Series switch is still connected to the switch port, it will no longer be part of the AMF network.

**Syntax** `switchport atmf-agentlink`  
`no switchport atmf-agentlink`

**Default** By default, no agent links exist and x600 Series switches are not visible to AMF networks.

**Mode** Interface mode for a switch port. Note that the link between the x600 and the AMF network must be a single link, not an aggregated link.

**Usage notes** The x600 Series switch provides the following information to the AMF node that it is connected to:

- The MAC address
- The IPv4 address
- The IPv6 address
- The name/type of the device (Allied Telesis x600)
- The name of the current firmware
- The version of the current firmware
- The configuration name

AMF guestnode also makes most of this information available from x600 Series switches, but requires configuration with DHCP and/or LLDP. AMF agent is simpler; as soon the x600 is connected to an appropriately configured port of an AMF node, it is immediately integrated into the AMF network.

To see information about the x600 Series switch, use the **show atmf links guest detail** command.

**Example** To configure port1.0.1 as an agent link, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport atmf-agentlink
```

**Related commands** [show atmf links guest](#)

# switchport atmf-arealink remote-area

**Overview** This command enables you to configure a port or aggregator to be an AMF arealink. AMF arealinks are designed to operate between two nodes in different areas in an AMF network.

Use the **no** variant of this command to remove any AMF-arealink that may exist for the selected port or aggregated link.

This command is only available on AMF controllers and master nodes.

**Syntax** `switchport atmf-arealink remote-area <area-name> vlan <2-4094>`  
`no switchport atmf-arealink`

| Parameter   | Description  |
|-------------|--|
| <area-name> | The name of the remote area that the port is connecting to.  |
| <2-4094>    | The VLAN ID for the link. This VLAN cannot be used for any other purpose, and the same VLAN ID must be used at each end of the link. |

**Default** By default, no arealinks are configured

**Mode** Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

**Usage notes** Run this command on the port or aggregator at both ends of the link.

Each area must have the area-name configured, and the same area password must exist on both ends of the link.

Running this command will automatically place the port or static aggregator into trunk mode (i.e. switchport mode trunk) and will synchronize the area information stored on the two nodes.

You can configure multiple arealinks between two area nodes, but only one arealink at any time will be in use. All other arealinks will block information, to prevent network storms.

**Example** To make switchport port1.0.2 an arealink to the *Auckland* area on VLAN 6, use the following commands

```
controller-1# configure terminal
controller-1(config)# interface port1.0.2
controller-1(config-if)# switchport atmf-arealink remote-area
Auckland vlan 6
```

**Related  
commands** [atmf area](#)  
[atmf area password](#)  
[atmf virtual-link](#)  
[show atmf links](#)

# switchport atmf-crosslink

**Overview** This command configures the selected port, statically aggregated link or dynamic channel group (LACP) to be an AMF crosslink. Running this command will automatically place the port or aggregator into trunk mode (i.e. **switchport mode trunk**).

The connection between two AMF masters must utilize a crosslink. Crosslinks are used to carry the AMF control information between master nodes. Multiple crosslinks can be configured between two master nodes, but only one crosslink can be active at any particular time. All other crosslinks between masters will be placed in the blocking state, in order to prevent broadcast storms.

Use the **no** variant of this command to remove any crosslink that may exist for the selected port or aggregated link.

**Syntax** `switchport atmf-crosslink`  
`no switchport atmf-crosslink`

**Mode** Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

**Usage notes** Crosslinks can be used anywhere within an AMF network. They have the effect of separating the AMF network into separate domains.

Where this command is used, it is also good practice to use the **switchport trunk native vlan** command with the parameter **none** selected. This is to prevent a network storm on a topology of ring connected devices.

**Example 1** To make switchport port1.0.1 an AMF crosslink, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# switchport atmf-crosslink
```

**Example 2** This example is shown twice. Example 2A is the most basic command sequence. Example 2B is a good practice equivalent that avoids problems such as broadcast storms that can otherwise occur.

**Example 2A** To make static aggregator sa1 an AMF crosslink, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface sa1
Node_1(config-if)# switchport atmf-crosslink
```



**Example 2B** To make static aggregator sa1 an AMF crosslink, use the following commands for good practice:

```
Node_1# configure terminal
Node_1(config)# interface sa1
Node_1(config-if)# switchport atmf-crosslink
Node_1(config-if)# switchport trunk allowed vlan add 2
Node_1(config-if)# switchport trunk native vlan none
```

In this example VLAN 2 is assigned to the static aggregator, and the native VLAN (VLAN 1) is explicitly excluded from the aggregated ports and the crosslink assigned to it.

**NOTE:** *The AMF management and domain VLANs are automatically added to the aggregator and the crosslink.*

**Related commands** [show atmf links statistics](#)

# switchport atmf-guestlink

**Overview** Guest links are used to provide basic AMF functionality to non AMF capable devices. Guest links can be configured for either a selected switch port or a range of switch ports and use generic protocols to collect status and configuration information that the guest devices make available.

Use the **no** variant of this command to remove the guest node functionality from the selected port or ports.

**NOTE:** AMF guest nodes are not supported on ports using the OpenFlow protocol.

**Syntax** `switchport atmf-guestlink [class <guest-class>] [ip <A.B.C.D> | ipv6 <X:X::X:X>]`  
`no switchport atmf-guestlink`

| Parameter     | Description   |
|---------------|---|
| class         | Set a guest class   |
| <guest-class> | The name of the guest class.                                  |
| ip            | Specifies that the address following will have an IPv4 format |
| <A.B.C.D>     | The guest node's IP address in IPv4 format.                   |
| ipv6          | Specifies that the address following will have an IPv6 format |
| <X:X::X:X>    | The guest node's IP address in IPv6 format.                   |

**Default** No guest links are configured.

**Mode** Interface

**Example 1** To configure switchport port1.0.1 to be a guest link, that will connect to a guest node having a guest class of **camera** and an IPv4 address of **192.168.3.3**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink class camera ip
192.168.3.3
```

**Example 2** To configure switchport port1.0.1 to be a guest link, which will connect to a guest node having a guest class of **phone** and an IPv6 address of **2001:db8:21e:10d::5**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink class phone ipv6
2000:db8:21e:10d::5
```

**Example 3** To configure switchport port1.0.1 to be a guest link, using the default model type and learning method address, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink
```

**Example 4** To configure switchports port1.0.1 to port1.0.3 to be guest links, for the guest class **camera**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1-port1.0.3
node1(config-if)# switchport atmf-guestlink class camera
```

**Example 5** To remove the guest-link functionality from switchport port1.0.1, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# no switchport atmf-guestlink
```

**Related commands**

- atmf guest-class
- discovery
- http-enable
- username
- modeltype
- show atmf links guest
- show atmf guests

# switchport atmf-link

**Overview** This command enables you to configure a port or aggregator to be an AMF up/down link. Running this command will automatically place the port or aggregator into trunk mode. If the port was previously configured in access mode, the configured access VLAN will be removed.

Use the **no** variant of this command to remove any AMF-link that may exist for the selected port or aggregated link.

**Syntax** `switchport atmf-link`  
`no switchport atmf-link`

**Mode** Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

**Usage notes** Up/down links and virtual links interconnect domains in a vertical hierarchy, with the highest domain being the core domain. In effect, they form a tree of interconnected AMF domains. This tree must be loop-free. Therefore, you must configure your links so that no rings are formed only from up/down links and/or virtual links.

Within each domain, cross-links between AMF nodes define those nodes as siblings within the same domain. You can form rings by combining cross-links with up/down links and/or virtual links, as long as each AMF domain links upwards to only a single parent domain. Each domain may link downwards to multiple child domains.

**Example** To make switchport port1.0.1 an AMF up/down link, 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}

| Parameter | Description           |
|-----------|-----------------------|
| join      | AMF node join event.  |
| leave     | AMF node leave event. |

**Mode** Trigger Configuration

**CAUTION:** Only configure this trigger on one device because it is a network wide event.

**Example 1** To configure trigger 5 to activate at an AMF node leave event, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger) type atmf node leave
```

**Example 2** The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
=====
node1, node2, node3:
=====

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

### Display the trigger configurations

AMF-Net[3]# show trigger

This command returns the following display:

```
=====
node1:
=====

TR# Type & Details      Description          Ac Te Tr Repeat      #Scr Days/Date
-----
001 Periodic (2 min)    Periodic Status Chk Y  N  Y Continuous    1  smtwtfS
005 ATMF node (leave)  E-mail on ATMF Exit Y  N  Y Continuous    1  smtwtfS
-----

=====
Node2, Node3,
=====

TR# Type & Details      Description          Ac Te Tr Repeat      #Scr Days/Date
-----
005 ATMF node (leave)  E-mail on ATMF Exit Y  N  Y Continuous    1  smtwtfS
-----
```

### Display the triggers configured on each of the nodes in the AMF Network.

AMF-Net[3]# show running-config trigger

This command returns the following display:

```
=====
Node1:
=====

trigger 1
  type periodic 2
  script 1 atmf.scp
trigger 5
  type atmf node leave
  description "E-mail on ATMF Exit"
  script 1 email_me.scp
!

=====
Node2, Node3:
=====

trigger 5
  type atmf node leave
  description "E-mail on ATMF Exit"
  script 1 email_me.scp
!
```

**Related  
commands** [show trigger](#)

# undebbug atmf

**Overview** This command is an alias for the **no** variant of the [debug atmf](#) command.



# username

**Overview** This command enables you to assign a **username** to a guest class. Guests may require a username and possibly also a password. In its non-encrypted form the password must be between 1 and 32 characters and will allow spaces. In its encrypted form the password must be between 1 to 64 characters and will allow any character

**Syntax** `username <NAME> password [8] <USERPASS>`  
`no username`

| Parameter  | Description  |
|------------|--|
| username   | Indicates that a user name is to follow  |
| <NAME>     | User name of the guest node  |
| password   | Indicates that a password (or specifier) is to follow.   |
| 8          | Specifier indicating that the following password is encrypted. It's primary purpose is to differentiate between the configuration input and the CLI input. You should not specify this for CLI input |
| <USERPASS> | The password to be entered for the guest node.   |

**Default** No usernames configured

**Mode** AMF Guest Configuration Mode

**Example 1** To assign the user name **reception** and the password of **secret** to an AMF guest node that has the guest class of **phone1** use the following commands:

```
node1# conf t
node1(config)# amf guest-class phone1
node1(config-atmf-guest)# username reception password secret
node1(config-atmf-guest)# end
```

**Example 2** To remove a guest node username and password for the user guest class **phone1**, use the following commands:

```
node1# conf t
node1(config)# atmf guest-class phone1
node1(config-atmf-guest)# no username
node1(config-atmf-guest)# end
```

**Related commands** [show atmf links detail](#)  
[atmf guest-class](#)  
[switchport atmf-guestlink](#)

show atmf links guest

show atmf nodes

# 20

# Dynamic Host Configuration Protocol (DHCP) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure DHCP.

Note that the DHCP client does not support tunnel interfaces.

For more information, see the [DHCP Feature Overview and Configuration Guide](#), which is available at the above link on alliedtelesis.com.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#). This guide is available at the above link on alliedtelesis.com.

- Command List**
- [“bootfile”](#) on page 901
  - [“clear ip dhcp binding”](#) on page 902
  - [“default-router”](#) on page 903
  - [“dns-server”](#) on page 904
  - [“domain-name”](#) on page 905
  - [“host \(DHCP\)”](#) on page 906
  - [“ip address dhcp”](#) on page 907
  - [“ip dhcp bootp ignore”](#) on page 909
  - [“ip dhcp leasequery enable”](#) on page 910
  - [“ip dhcp option”](#) on page 911
  - [“ip dhcp pool”](#) on page 913
  - [“ip dhcp-client default-route distance”](#) on page 914
  - [“ip dhcp-client request vendor-identifying-specific”](#) on page 916
  - [“ip dhcp-client vendor-identifying-class”](#) on page 917
  - [“ip dhcp-relay agent-option”](#) on page 918

- [“ip dhcp-relay agent-option checking”](#) on page 920
- [“ip dhcp-relay agent-option remote-id”](#) on page 922
- [“ip dhcp-relay information policy”](#) on page 924
- [“ip dhcp-relay maxhops”](#) on page 926
- [“ip dhcp-relay max-message-length”](#) on page 927
- [“ip dhcp-relay server-address”](#) on page 929
- [“ip dhcp-relay use-client-side-address”](#) on page 931
- [“lease”](#) on page 933
- [“network \(DHCP\)”](#) on page 935
- [“next-server”](#) on page 936
- [“option”](#) on page 937
- [“probe enable”](#) on page 939
- [“probe packets”](#) on page 940
- [“probe timeout”](#) on page 941
- [“probe type”](#) on page 942
- [“range”](#) on page 943
- [“route”](#) on page 944
- [“service dhcp-relay”](#) on page 945
- [“service dhcp-server”](#) on page 946
- [“short-lease-threshold”](#) on page 947
- [“show counter dhcp-client”](#) on page 949
- [“show counter dhcp-relay”](#) on page 950
- [“show counter dhcp-server”](#) on page 953
- [“show dhcp lease”](#) on page 955
- [“show ip dhcp binding”](#) on page 956
- [“show ip dhcp pool”](#) on page 958
- [“show ip dhcp-relay”](#) on page 963
- [“show ip dhcp server statistics”](#) on page 964
- [“show ip dhcp server summary”](#) on page 966
- [“subnet-mask”](#) on page 967

# bootfile

**Overview** This command sets the boot filename for a DHCP server pool. This is the name of the boot file that the client should use in its bootstrap process. It may need to include a path.

The **no** variant of this command removes the boot filename from a DHCP server pool.

**Syntax** bootfile <filename>  
no bootfile

| Parameter  | Description         |
|------------|---------------------|
| <filename> | The boot file name. |

**Mode** DHCP Configuration

**Example** To configure the boot filename for a pool P2, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# bootfile boot/main_boot.bt
```

# clear ip dhcp binding

**Overview** This command clears either a specific lease binding or the lease bindings specified by the command or DHCP server. The command will only take effect on dynamically allocated bindings, not statically configured bindings.

**Syntax** `clear ip dhcp binding {ip <ip-address>|mac <mac-address>|all|pool <pool-name>|range <low-ip-address> <high-ip-address>}`

| Parameter  | Description  |
|--|--|
| <code>ip &lt;ip-address&gt;</code>                               | IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D.   |
| <code>mac &lt;mac-address&gt;</code>                             | MAC address of the DHCP client, in hexadecimal notation in the format HHHH.HHHH.HHHH.  |
| <code>all</code>   | All DHCP bindings.   |
| <code>pool &lt;pool-name&gt;</code>                              | Description used to identify DHCP server address pool. Valid characters are any printable character. If the name contains spaces then you must enclose these in "quotation marks". |
| <code>range&lt;low-ip-address&gt; &lt;high-ip-address&gt;</code> | IPv4 address range for DHCP clients, in dotted decimal notation. The first IP address is the low end of the range, the second IP address is the high end of the range.             |

**Mode** User Exec and Privileged Exec

**Usage** A specific binding may be deleted by **ip** address or **mac** address, or several bindings may be deleted at once using **all**, **pool** or **range**.

Note that if you specify to clear the **ip** or **mac** address of what is actually a static DHCP binding, an error message is displayed. If **all**, **pool** or **range** are specified and one or more static DHCP bindings exist within those addresses, any dynamic entries within those addresses are cleared but any static entries are not cleared.

**Examples** To clear the specific IP address binding 192.168.1.1, use the command:

```
awplus# clear ip dhcp binding ip 192.168.1.1
```

To clear all dynamic DHCP entries, use the command:

```
awplus# clear ip dhcp binding all
```

**Related commands** [show ip dhcp binding](#)

# default-router

**Overview** This command adds a default router to the DHCP address pool you are configuring. You can use this command multiple times to create a list of default routers on the client's subnet. This sets the router details using the pre-defined option 3. Note that if you add a user-defined option 3 using the **option** command, then you will override any settings created with this command.

The **no** variant of this command removes either the specified default router, or all default routers from the DHCP pool.

**Syntax** `default-router <ip-address>`  
`no default-router [<ip-address>]`

| Parameter                       | Description   |
|---------------------------------|---|
| <code>&lt;ip-address&gt;</code> | IPv4 address of the default router, in dotted decimal notation. |

**Mode** DHCP Configuration

**Examples** To add a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# default-router 192.168.1.2
```

To remove a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router 192.168.1.2
```

To remove all routers from the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router
```

# dns-server

**Overview** This command adds a Domain Name System (DNS) server to the DHCP address pool you are configuring. You can use this command multiple times to create a list of DNS name servers available to the client. This sets the DNS server details using the pre-defined option 6.

Note that if you add a user-defined option 6 using the [option](#) command, then you will override any settings created with this command.

The **no** variant of this command removes either the specified DNS server, or all DNS servers from the DHCP pool.

**Syntax** `dns-server <ip-address>`  
`no dns-server [<ip-address>]`

| Parameter                       | Description   |
|---------------------------------|---|
| <code>&lt;ip-address&gt;</code> | IPv4 address of the DNS server, in dotted decimal notation. |

**Mode** DHCP Configuration

**Examples** To add the DNS server with the assigned IP address 192.168.1.1 to the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# dns-server 192.168.1.1
```

To remove the DNS server with the assigned IP address 192.168.1.1 from the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no dns-server 192.168.1.1
```

To remove all DNS servers from the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no dns-server
```

**Related commands**

- [default-router](#)
- [option](#)
- [service dhcp-server](#)
- [show ip dhcp pool](#)
- [subnet-mask](#)



# domain-name

**Overview** This command adds a domain name to the DHCP address pool you are configuring. Use this command to specify the domain name that a client should use when resolving host names using the Domain Name System. This sets the domain name details using the pre-defined option 15.

Note that if you add a user-defined option 15 using the [option](#) command, then you will override any settings created with this command.

The **no** variant of this command removes the domain name from the address pool.

**Syntax** `domain-name <domain-name>`  
`no domain-name`

| Parameter                        | Description  |
|----------------------------------|--|
| <code>&lt;domain-name&gt;</code> | The domain name you wish to assign the DHCP pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks". |

**Mode** DHCP Configuration

**Examples** To add the domain name `Nerv_Office` to DHCP pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# domain-name Nerv_Office
```

To remove the domain name `Nerv_Office` from DHCP pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no domain-name Nerv_Office
```

**Related commands**

- [default-router](#)
- [dns-server](#)
- [option](#)
- [service dhcp-server](#)
- [show ip dhcp pool](#)
- [subnet-mask](#)

# host (DHCP)

**Overview** This command adds a static host address to the DHCP address pool you are configuring. The client with the matching MAC address is permanently assigned this IP address. No other clients can request it.

The **no** variant of this command removes the specified host address from the DHCP pool. Use the **no host all** command to remove all static host addresses from the DHCP pool.

**Syntax** `host <ip-address> <mac-address>`  
`no host <ip-address>`  
`no host all`

| Parameter                        | Description  |
|----------------------------------|--|
| <code>&lt;ip-address&gt;</code>  | IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D    |
| <code>&lt;mac-address&gt;</code> | MAC address of the DHCP client, in hexadecimal notation in the format HHHH.HHHH.HHHH |

**Mode** DHCP Configuration

**Usage** Note that a network/mask must be configured using a **network** command before issuing a **host** command. Also note that a host address must match a network to add a static host address.

**Examples** To add the host at 192.168.1.5 with the MAC address 000a.451d.6e34 to DHCP pool 1, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool 1
awplus(dhcp-config)# network 192.168.1.0/24
awplus(dhcp-config)# host 192.168.1.5 000a.451d.6e34
```

To remove the host at 192.168.1.5 with the MAC address 000a.451d.6e34 from DHCP pool 1, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool 1
awplus(dhcp-config)# no host 192.168.1.5 000a.451d.6e34
```

**Related Commands** [lease](#)  
[range](#)  
[show ip dhcp pool](#)

# ip address dhcp

**Overview** This command activates the DHCP client on the interface you are configuring. This allows the interface to use the DHCP client to obtain its IP configuration details from a DHCP server on its connected network.

The **client-id** and **hostname** parameters are identifiers that you may want to set in order to interoperate with your existing DHCP infrastructure. If neither option is needed, then the DHCP server uses the MAC address field of the request to identify the host.

The DHCP client supports the following IP configuration options:

- Option 1 - the subnet mask for your device.
- Option 3 - a list of default routers.
- Option 6 - a list of DNS servers. This list appends the DNS servers set on your device with the [ip name-server](#) command.
- Option 15 - a domain name used to resolve host names. This option replaces the domain name set with the [ip domain-name](#) command. Your device ignores this domain name if it has a domain list set using the [ip domain-list](#) command.
- Option 51 - lease expiration time.

The **no** variant of this command stops the interface from obtaining IP configuration details from a DHCP server.

**Syntax** `ip address dhcp [client-id <interface>] [hostname <hostname>]`  
`no ip address dhcp`

| Parameter  | Description  |
|--|--|
| <code>client-id</code><br><code>&lt;interface&gt;</code> | The name of the interface you are activating the DHCP client on. If you specify this, then the MAC address associated with the specified interface is sent to the DHCP server in the optional identifier field.<br>Default: no default |
| <code>hostname</code><br><code>&lt;hostname&gt;</code>   | The hostname for the DHCP client on this interface. Typically this name is provided by the ISP.<br>Default: no default   |

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Examples** To set the interface `vlan1` to use DHCP to obtain an IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip address dhcp
```

To stop the interface vlan1 from using DHCP to obtain its IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip address dhcp
```

**Related commands**

- [ip address \(IP Addressing and Protocol\)](#)
- [show ip interface](#)
- [show running-config](#)

# ip dhcp bootp ignore

**Overview** This command configures the DHCP server to ignore any BOOTP requests it receives. The DHCP server accepts BOOTP requests by default.

The **no** variant of this command configures the DHCP server to accept BOOTP requests. This is the default setting.

**Syntax** ip dhcp bootp ignore  
no ip dhcp bootp ignore

**Mode** Global Configuration

**Examples** To configure the DHCP server to ignore BOOTP requests, use the commands:

```
awplus# configure terminal  
awplus(config)# ip dhcp bootp ignore
```

To configure the DHCP server to respond to BOOTP requests, use the commands:

```
awplus# configure terminal  
awplus(config)# no ip dhcp bootp ignore
```

**Related commands** [show ip dhcp server summary](#)

# ip dhcp leasequery enable

**Overview** Use this command to enable the DHCP server to respond to DHCPLEASEQUERY packets. Enabling the DHCP leasequery feature allows a DHCP Relay Agent to obtain IP address information directly from the DHCP server using DHCPLEASEQUERY messages.

Use the **no** variant of this command to disable the support of DHCPLEASEQUERY packets.

For more information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** ip dhcp leasequery enable  
no ip dhcp leasequery enable

**Default** DHCP leasequery support is disabled by default.

**Mode** Global Configuration

**Examples** To enable DHCP leasequery support, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp leasequery enable
```

To disable DHCP leasequery support, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp leasequery enable
```

**Related commands** [show counter dhcp-server](#)  
[show ip dhcp server statistics](#)  
[show ip dhcp server summary](#)

# ip dhcp option

**Overview** This command creates a user-defined DHCP option. Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

You can use this option when configuring a DHCP pool, by using the [option](#) command.

The **no** variant of this command removes either the specified user-defined option, or removes all user-defined options. This also automatically removes the user-defined options from the associated DHCP address pools.

**Syntax** `ip dhcp option <1-254> [name <option-name>] [<option-type>]`  
`no ip dhcp option [<1-254>|<option-name>]`

| Parameter     | Description  |       |                      |     |   |    |   |         |                                |      |   |
|---------------|--|-------|----------------------|-----|---|----|---|---------|--------------------------------|------|---|
| <1-254>       | The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.   |       |                      |     |   |    |   |         |                                |      |   |
| <option-name> | Option name used to identify the option. You cannot use a number as the option name. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".<br>Default: no default   |       |                      |     |   |    |   |         |                                |      |   |
| <option-type> | The option value. You must specify a value that is appropriate to the option type: <table border="1" data-bbox="678 1288 1422 1794"> <tbody> <tr> <td>ascii</td> <td>An ASCII text string</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 by 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 that either sets (to 1) or unsets (to 0) a flag: <b>true</b>, <b>on</b>, or <b>enabled</b> will set the flag. <b>false</b>, <b>off</b> or <b>disabled</b> will unset the flag.</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: <b>true</b> , <b>on</b> , or <b>enabled</b> will set the flag. <b>false</b> , <b>off</b> or <b>disabled</b> will unset the flag. |
| ascii         | An ASCII text string   |       |                      |     |   |    |   |         |                                |      |   |
| hex           | A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.  |       |                      |     |   |    |   |         |                                |      |   |
| ip            | An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually by using the option command multiple times.  |       |                      |     |   |    |   |         |                                |      |   |
| integer       | A number from 0 to 4294967295.   |       |                      |     |   |    |   |         |                                |      |   |
| flag          | A value that either sets (to 1) or unsets (to 0) a flag: <b>true</b> , <b>on</b> , or <b>enabled</b> will set the flag. <b>false</b> , <b>off</b> or <b>disabled</b> will unset the flag.  |       |                      |     |   |    |   |         |                                |      |   |

**Mode** Global Configuration

**Examples** To define a user-defined ASCII string option as option 66, without a name, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp option 66 ascii
```

To define a user-defined hexadecimal string option as option 46, with the name "tcpip-node-type", use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp option 46 name tcpip-node-type hex
```

To define a user-defined IP address option as option 175, with the name special-address, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp option 175 name special-address ip
```

To remove the specific user-defined option with the option number 12, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option 12
```

To remove the specific user-defined option with the option name perform-router-discovery, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option perform-router-discovery
```

To remove all user-defined option definitions, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option
```

**Related commands**

[default-router](#)  
[dns-server](#)  
[domain-name](#)  
[option](#)  
[service dhcp-server](#)  
[show ip dhcp server summary](#)  
[subnet-mask](#)



# ip dhcp pool

**Overview** This command will enter the configuration mode for the pool name specified. If the name specified is not associated with an existing pool, the device will create a new pool with this name, then enter the configuration mode for the new pool.

Once you have entered the DHCP configuration mode, all commands executed before the next **exit** command will apply to this pool.

You can create multiple DHCP pools on devices with multiple interfaces. This allows the device to act as a DHCP server on multiple interfaces to distribute different information to clients on the different networks.

The **no** variant of this command deletes the specific DHCP pool.

**Syntax** `ip dhcp pool <pool-name>`  
`no ip dhcp pool <pool-name>`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;pool-name&gt;</code> | Description used to identify this DHCP pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks". |

**Mode** Global Configuration

**Example** To create the DHCP pool named P2 and enter DHCP Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)#
```

To delete the DHCP pool named P2, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp pool P2
```

**Related commands** [service dhcp-server](#)

# ip dhcp-client default-route distance

**Overview** Use this command to specify an alternative Administrative Distance (AD) for the current default route (from DHCP) for an interface.

Use the **no** variant of this command to set the AD back to the default of 1.

**Syntax** `ip dhcp-client default-route distance [<1-255>]`  
`no ip dhcp-client default-route distance`

| Parameter | Description   |
|-----------|---|
| <1-255>   | Administrative Distance (AD) from the range 1 though 255. |

**Default** 1

**Mode** Interface Configuration

**Usage notes** DHCP client interfaces can automatically add a default route with an AD of 1 into the IP Routing Information Base (RIB).

Any pre-existing default route(s) via alternative interfaces (configured with a higher AD) will no longer be selected as the preferred forwarding path for traffic when the DHCP based default route is added to the IP routing table.

This can be problematic if the DHCP client is operating via an interface that is only intended to be used for back-up interface redundancy purposes, such as a VLAN containing a single switchport, or a 4G cellular interface on an AR-Series Firewall.

Use this command to set the AD of the default route (via a specific DHCP client interface) to a non-default (higher cost) value, ensuring any pre-existing default route(s) via any other interface(s) continue to be selected as the preferred forwarding path for network traffic.

When the command is used, the static default route is deleted from the RIB, the distance value of the route is modified to the configured distance value, then it is reinstalled into the RIB.

**Examples** To set the AD for the default route added by DHCP via cellular interface wwan0 to 150, use the commands:

```
awplus# configure terminal
awplus(config)# interface wwan0
awplus(config-if)# ip dhcp-client default-route distance 150
```

To set the AD for the default route back to the default value of 1, use the commands:

```
awplus# configure terminal
awplus(config)# interface wwan0
awplus(config-if)# no ip dhcp-client default-route distance
```

**Related commands** [show ip route](#)  
[show ip route database](#)

**Command changes** Version 5.4.7-0.2 Command added.

# ip dhcp-client request vendor-identifying-specific

**Overview** Use this command to add vendor-identifying vendor-specific information (option 125) requests to the DHCP discovery packets sent by an interface. This option, along with option 124, can be used to send vendor specific information back to a DHCP client.

See RFC3925 for more information on Vendor-Identifying Vendor Options for DHCPv4.

Use the **no** variant of this command to remove the vendor-identifying-specific request from an interface.

**Syntax** `ip dhcp-client request vendor-identifying-specific`  
`no ip dhcp-client request vendor-identifying-specific`

**Default** The vendor-identifying-specific request is not configured by default.

**Mode** Interface Configuration

**Usage notes** The DHCP client must be activated on the interface, using the [ip address dhcp](#) command, so that DHCP discovery packets are sent.

**Example** To add the vendor-identifying-specific request on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-client request
vendor-identifying-specific
```

To remove the vendor-identifying-specific request on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-client request
vendor-identifying-specific
```

**Related commands** [ip address dhcp](#)  
[ip dhcp-client vendor-identifying-class](#)

**Command changes** Version 5.4.7-2.1: command added

# ip dhcp-client vendor-identifying-class

**Overview** Use this command to add a vendor-identifying vendor class (option 124) to the DHCP discovery packets sent by an interface. This option places the Allied Telesis Enterprise number (207) into the discovery packet. Option 124, along with option 125, can be used to send vendor specific information back to a DHCP client.

See RFC3925 for more information on Vendor-Identifying Vendor Options for DHCPv4.

Use the **no** variant of this command to remove the vendor-identifying-class from an interface.

**Syntax** `ip dhcp-client vendor-identifying-class`  
`no ip dhcp-client vendor-identifying-class`

**Default** The vendor-identifying-class is not configured by default.

**Mode** Interface Configuration

**Usage notes** The DHCP client must be activated on the interface, using the [ip address dhcp](#) command, so that DHCP discovery packets are sent.

**Example** To remove the vendor-identifying-specific request on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-client vendor-identifying-class
```

**Related commands** [ip address dhcp](#)  
[ip dhcp-client request vendor-identifying-specific](#)

**Command changes** Version 5.4.7-2.1: command added

# ip dhcp-relay agent-option

**Overview** This command enables the DHCP Relay Agent to insert the DHCP Relay Agent Information Option (Option 82) into the client-request packets that it relays to its DHCP server. This allows the DHCP Relay Agent to pass on information to the server about the network location of the client device. The DHCP Relay Agent strips the DHCP Relay Agent Option 82 field out of the DHCP server's response, so that the DHCP client never sees this field.

When the DHCP Relay Agent appends its DHCP Relay Agent Option 82 data into the packet, it first overwrites any pad options present; then if necessary, it increases the packet length to accommodate the DHCP Relay Agent Option 82 data.

The **no** variant of this command stops the DHCP Relay Agent from appending the Option 82 field onto DHCP requests before forwarding it to the server.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**NOTE:** *The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands `ip dhcp-relay agent-option` and `ip dhcp-relay information policy` have been configured.*

**Syntax** `ip dhcp-relay agent-option`  
`no ip dhcp-relay agent-option`

**Default** DHCP Relay Agent Information Option (Option 82) insertion is disabled by default.

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** Use this command to alter the DHCP Relay Agent Option 82 setting when your device is the first hop for the DHCP client. To limit the maximum length of the packet, use the [ip dhcp-relay max-message-length](#) command.

**Examples** To make the DHCP Relay Agent listening on vlan1 append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the DHCP Relay Agent from appending the DHCP Relay Agent Option 82 field on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay agent-option
```

To make the relay agent listening on PPP interface ppp0 append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the relay agent from appending the DHCP Relay Agent Option 82 field on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip dhcp-relay agent-option
```

**Related commands**

- [ip dhcp-relay agent-option remote-id](#)
- [ip dhcp-relay information policy](#)
- [ip dhcp-relay max-message-length](#)
- [service dhcp-relay](#)

# ip dhcp-relay agent-option checking

**Overview** This command enables the DHCP Relay Agent to check DHCP Relay Agent Information Option (Option 82) information in response packets returned from DHCP servers. If the information does not match the information it has for its own client (downstream) interface then the DHCP Relay Agent drops the packet. Note that [ip dhcp-relay agent-option](#) must be configured.

The DHCP Relay Agent Option 82 field is included in relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled ([ip dhcp-relay agent-option](#)), and
- DHCP Relay Agent is enabled on the device ([service dhcp-relay](#))

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay agent-option checking`  
`no ip dhcp-relay agent-option checking`

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Examples** To make the DHCP Relay Agent listening on vlan1 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay agent-option
awplus(config-if)# ip dhcp-relay agent-option checking
```

To stop the DHCP Relay Agent on vlan1 from checking the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay agent-option checking
```

To make the relay agent listening on PPP interface ppp0 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip dhcp-relay agent-option
awplus(config-if)# ip dhcp-relay agent-option checking
```

To stop the relay agent from checking the DHCP Relay Agent Information Option (Option 82) field on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip dhcp-relay agent-option checking
```



**Related commands**

- ip dhcp-relay agent-option
- ip dhcp-relay agent-option remote-id
- ip dhcp-relay information policy
- service dhcp-relay

# ip dhcp-relay agent-option remote-id

**Overview** Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field the DHCP Relay Agent inserts into clients' request packets. The Remote ID identifies the device that is inserting the DHCP Relay Agent Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the device's MAC address.

Use the **no** variant of this command to return the Remote ID for an interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay agent-option remote-id <remote-id>`  
`no ip dhcp-relay agent-option remote-id`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;remote-id&gt;</code> | An alphanumeric (ASCII) string, 1 to 63 characters in length. Additional characters allowed are hyphen (-), underscore (_) and hash (#). Spaces are not allowed. |

**Default** The Remote ID is set to the device's MAC address by default.

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled ([ip dhcp-relay agent-option](#)), and
- DHCP Relay Agent is enabled on the device ([service dhcp-relay](#))

**Examples** To set the Remote ID to myid for client DHCP packets received on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay agent-option remote-id
```

To set the Remote ID to myid for client DHCP packets received on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0 timeslots all
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0 timeslots all
awplus(config-if)# no ip dhcp-relay agent-option remote-id
```

**Related commands**

- [ip dhcp-relay agent-option](#)
- [ip dhcp-relay agent-option checking](#)
- [show ip dhcp-relay](#)

# ip dhcp-relay information policy

**Overview** This command sets the policy for how the DHCP relay deals with packets arriving from the client that contain DHCP Relay Agent Option 82 information.

If the command **ip dhcp-relay agent-option** has not been configured, then this command has no effect at all - no alteration is made to Option 82 information in packets arriving from the client side.

However, if the command **ip dhcp-relay agent-option** has been configured, this command modifies how the DHCP relay service deals with cases where the packet arriving from the client side already contains DHCP Relay Agent Option 82 information.

This command sets the action that the DHCP relay should take when a received DHCP client request contains DHCP Relay Agent Option 82 information.

By default, the DHCP Relay Agent replaces any existing DHCP Relay Agent Option 82 field with its own DHCP Relay Agent field. This is equivalent to the functionality of the **replace** parameter.

The **no** variant of this command returns the policy to the default behavior - i.e. replacing the existing DHCP Relay Agent Option 82 field.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**NOTE:** The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands [ip dhcp-relay agent-option](#) and [ip dhcp-relay information policy](#) have been configured.

**Syntax** `ip dhcp-relay information policy {append|drop|keep|replace}`  
`no ip dhcp-relay information policy`

| Parameter | Description  |
|-----------|--|
| append    | The DHCP Relay Agent appends the DHCP Relay Agent Option 82 field of the packet with its own DHCP Relay Agent Option 82 details.                               |
| drop      | The DHCP Relay Agent discards the packet.  |
| keep      | The DHCP Relay Agent forwards the packet without altering the DHCP Relay Agent Option 82 field.  |
| replace   | The DHCP Relay Agent replaces the existing DHCP Relay Agent details in the DHCP Relay Agent Option 82 field with its own details before forwarding the packet. |

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Examples** To make the DHCP Relay Agent listening on vlan1 drop any client requests that already contain DHCP Relay Agent Option 82 information, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay information policy drop
```

To reset the DHCP relay information policy to the default policy for interface vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay information policy
```

**Related commands**

- [ip dhcp-relay agent-option](#)
- [ip dhcp-relay agent-option checking](#)
- [service dhcp-server](#)

# ip dhcp-relay maxhops

**Overview** This command sets the hop count threshold for discarding BOOTP messages. When the hops field in a BOOTP message exceeds the threshold, the DHCP Relay Agent discards the BOOTP message. The hop count threshold is set to 10 hops by default.

Use the **no** variant of this command to reset the hop count to the default.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay maxhops <1-255>`  
`no ip dhcp-relay maxhops`

| Parameter | Description                  |
|-----------|------------------------------|
| <1-255>   | The maximum hop count value. |

**Default** The default hop count threshold is 10 hops.

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Example** To set the maximum number of hops to 5 for packets received on interface vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay maxhops 5
```

**Related commands** [service dhcp-relay](#)

# ip dhcp-relay max-message-length

**Overview** This command applies when the device is acting as a DHCP Relay Agent and DHCP Relay Agent Option 82 insertion is enabled. It sets the maximum DHCP message length (in bytes) for the DHCP packet with its DHCP Relay Agent Option 82 data inserted. From this value it calculates the maximum packet size that it will accept at its input. Packets that arrive greater than this value will be dropped.

The **no** variant of this command sets the maximum message length to its default of 1400 bytes.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay max-message-length <548-1472>`  
`no ip dhcp-relay max-message-length`

| Parameter  | Description   |
|------------|---|
| <548-1472> | The maximum DHCP message length (this is the message header plus the inserted DHCP option fields in bytes). |

**Default** The default is 1400 bytes.

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** When a DHCP Relay Agent (that has DHCP Relay Agent Option 82 insertion enabled) receives a request packet from a DHCP client, it will append the DHCP Relay Agent Option 82 component data, and forward the packet to the DHCP server. The DHCP client will sometimes issue packets containing pad option fields that can be overwritten with Option 82 data.

Where there are insufficient pad option fields to contain all the DHCP Relay Agent Option 82 data, the DHCP Relay Agent will increase the packet size to accommodate the DHCP Relay Agent Option 82 data. If the new (increased) packet size exceeds that defined by the **maximum-message-length** parameter, then the DHCP Relay Agent will drop the packet.

**NOTE:** Before setting this command, you must first run the `ip dhcp-relay agent-option` command. This will allow the DHCP Relay Agent Option 82 fields to be appended.

**Example** To set the maximum DHCP message length to 1200 bytes for packets arriving in interface vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
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 vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay max-message-length
```

**Related commands** [service dhcp-relay](#)



# ip dhcp-relay server-address

**Overview** This command adds a DHCP server for the DHCP Relay Agent to forward client DHCP packets to on a particular interface. You can add up to five DHCP servers on each device interface that the DHCP Relay Agent is listening on.

The **no** variant of this command deletes the specified DHCP server from the list of servers available to the DHCP relay agent.

The **no ip dhcp-relay** command removes all DHCP relay settings from the interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax**

```
ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}

no ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}

no ip dhcp-relay
```

| Parameter          | Description   |
|--------------------|---|
| <ipv4-address>     | Specify the IPv4 address of the DHCP server for the DHCP Relay Agent to forward client DHCP packets to, in dotted decimal notation. The IPv4 address uses the format A.B.C.D. |
| <ipv6-address>     | Specify the IPv6 address of the DHCPv6 server for the DHCPv6 Relay Agent to forward client DHCP packets to, in hexadecimal notation.  |
| <server-interface> | Specify the interface name of the DHCPv6 server. It is only required for a DHCPv6 server with an IPv6 address.  |

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** For a DHCP server with an IPv6 address you must specify the interface for the DHCP server. See examples below for configuration differences between IPv4 and IPv6 DHCP relay servers.

See also the [service dhcp-relay](#) command to enable the DHCP Relay Agent on your device. The [ip dhcp-relay server-address](#) command defines a relay destination on an interface on the device, needed by the DHCP Relay Agent to relay DHCP client packets to a DHCP server.

**Examples** To enable the DHCP Relay Agent to relay DHCP packets on interface vlan1 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 vlan1
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 vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay server-address 192.0.2.200
```

To disable DHCP relay on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay
```

**Related commands** [service dhcp-relay](#)

# ip dhcp-relay use-client-side-address

**Overview** Use this command to configure DHCP-Relay to use the client-side interface (that is the interface receiving the DHCP client packets) IP address as the source address of the relayed DHCP packets.

Use the **no** variant of this command to disable the use of the client-side interface IP address as the source IP address for relayed DHCP packets.

**Syntax** `ip dhcp-relay use-client-side-address`  
`no ip dhcp-relay use-client-side-address`

| Parameter                            | Description   |
|--------------------------------------|---|
| <code>use-client-side-address</code> | Use the client side interface IP address as the source IP address for relayed DHCP packets. |

**Default** By default, the server-side interface IP address is used as the source IP address of DHCP relayed packets.

**Mode** Global Configuration

**Usage notes** In most cases, there are filters placed between the DHCP relay and DHCP server which only allow DHCP packets from the client subnet to the server and back. This command allows you to configure the DHCP relay so that the relay will use the IP address of the interface **receiving** clients DHCP requests to be used as the source IP address of the relayed DHCP packets.

**Example** To configure the client-side IP address as the source IP address of DHCP relayed packets, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp-relay use-client-side-address
```

**Output** Figure 20-1: Example output from **show ip dhcp-relay**

Note that the second line of the display output shows the status of the client-side address being enabled as the source IP address.

```
awplus#sh ip dhcp-relay

DHCP Relay Service is enabled
Use of client side address as source address is enabled

vlan1 is down, line protocol is down
Maximum hop count is 10
Maximum DHCP message length is 1400
Insertion of Relay Agent Option is disabled
Checking of Relay Agent Option is disabled
Insertion of Subscriber-ID auto-MAC is disabled
The Remote Id string for Relay Agent Option is 0000.0000.0000
Relay Information policy is to replace existing relay agent information
List of servers : 10.1.1.100
```

**Related commands** [ip dhcp-relay server-address](#)

**Command changes** Version 5.4.9-0.7: command added

# lease

**Overview** This command sets the expiration time for a leased address for the DHCP address pool you are configuring. The time set by the days, hours, minutes and seconds is cumulative. The minimum total lease time that can be configured is 20 seconds. The maximum total lease time that can be configured is 120 days.

Note that if you add a user-defined option 51 using the `option` command, then you will override any settings created with this command. Option 51 specifies a lease time of 1 day.

Use the **infinite** parameter to set the lease expiry time to infinite (leases never expire).

Use the **no** variant of this command to return the lease expiration time back to the default of one day.

**Syntax** `lease <days> <hours> <minutes> [<seconds>]`  
`lease infinite`  
`no lease`

| Parameter                    | Description  |
|------------------------------|--|
| <code>&lt;days&gt;</code>    | The number of days, from 0 to 120, that the lease expiry time is configured for.<br>Default: 1 |
| <code>&lt;hours&gt;</code>   | The number of hours, from 0 to 24, that the lease expiry time is configured for.<br>Default: 0 |
| <code>&lt;minutes&gt;</code> | The number of minutes, from 0 to 60, the lease expiry time is configured for.<br>Default: 0    |
| <code>&lt;seconds&gt;</code> | The number of seconds, from 0 to 60, the lease expiry time is configured for.                  |
| <code>infinite</code>        | The lease never expires.   |

**Default** The default lease time is 1 day.

**Mode** DHCP Configuration

**Examples** To set the lease expiration time for address pool P2 to 35 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# lease 0 0 35
```

To set the lease expiration time for the address pool `Nerv_Office` to 1 day, 5 hours, and 30 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# lease 1 5 30
```

To set the lease expiration time for the address pool `P3` to 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P3
awplus(dhcp-config)# lease 0 0 0 20
```

To set the lease expiration time for the pool to never expire, use the command:

```
awplus(dhcp-config)# lease infinite
```

To return the lease expiration time to the default of one day, use the command:

```
awplus(dhcp-config)# no lease
```

**Related  
commands**

[option](#)  
[service dhcp-server](#)  
[short-lease-threshold](#)

# network (DHCP)

**Overview** This command sets the network (subnet) that the DHCP address pool applies to. The **no** variant of this command removes the network (subnet) from the DHCP address pool.

**Syntax** network  
{<ip-subnet-address/prefix-length> | <ip-subnet-address/mask>}  
no network

| Parameter                         | Description  |
|-----------------------------------|--|
| <ip-subnet-address/prefix-length> | The IPv4 subnet address in dotted decimal notation followed by the prefix length in slash notation.        |
| <ip-subnet-address/mask>          | The IPv4 subnet address in dotted decimal notation followed by the subnet mask in dotted decimal notation. |

**Mode** DHCP Configuration

**Usage notes** This command will fail if it would make existing ranges invalid. For example, if they do not lie within the new network you are configuring.

The **no** variant of this command will fail if ranges still exist in the pool. You must remove all ranges in the pool before issuing a **no network** command to remove a network from the pool.

**Examples** To configure a network for the address pool P2, where the subnet is 192.0.2.5 and the mask is 255.255.255.0, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# network 192.0.2.5/24
```

or you can use dotted decimal notation instead of slash notation for the subnet-mask:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# network 192.0.2.5 255.255.255.0
```

**Related commands** [service dhcp-server](#)  
[subnet-mask](#)

## next-server

**Overview** This command sets the next server address for a DHCP server pool. It is the address of the next server that the client should use in its bootstrap process.

The **no** variant of this command removes the next server address from the DHCP address pool.

**Syntax** `next-server <ip-address>`  
`no next-server`

| Parameter                       | Description  |
|---------------------------------|--|
| <code>&lt;ip-address&gt;</code> | The server IP address, entered in dotted decimal notation. |

**Mode** DHCP Configuration

**Example** To set the next-server address for the address pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# next-server 192.0.2.2
```



# option

**Overview** This command adds a user-defined option to the DHCP address pool you are configuring. For the **hex**, **integer**, and **flag** option types, if the option already exists, the new option overwrites the existing option's value. Options with an **ip** type can hold a list of IP addresses or masks (i.e. entries that have the A.B.C.D address format), so if the option already exists in the pool, then the new IP address is added to the list of existing IP addresses.

Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

The **no** variant of this command removes the specified user-defined option from the DHCP pool, or all user-defined options from the DHCP pool.

**Syntax** `option [<1-254>|<option-name>] <option-value>`  
`no option [<1-254>|<option-value>]`

| Parameter      | Description   |     |   |    |  |         |                                |      |  |
|----------------|---|-----|---|----|--|---------|--------------------------------|------|--|
| <1-254>        | The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.  |     |   |    |  |         |                                |      |  |
| <option-name>  | Option name associated with the option.   |     |   |    |  |         |                                |      |  |
| <option-value> | The option value. You must specify a value that is appropriate to the option type: <table border="1" data-bbox="710 1261 1423 1751"> <tbody> <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> | hex | A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long. | ip | An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually using the option command multiple times. | integer | A number from 0 to 4294967295. | flag | A value of either true, on, or enabled to set the flag, or false, off or disabled to unset the flag. |
| hex            | A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.   |     |   |    |  |         |                                |      |  |
| ip             | An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually using the option command multiple times.  |     |   |    |  |         |                                |      |  |
| integer        | A number from 0 to 4294967295.  |     |   |    |  |         |                                |      |  |
| flag           | A value of either true, on, or enabled to set the flag, or false, off or disabled to unset the flag.  |     |   |    |  |         |                                |      |  |

**Mode** DHCP Configuration

**Examples** To add the ASCII-type option named `tftp-server-name` to the pool P2 and give the option the value `server1`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# option tftp-server-name server1
```

To add the hex-type option named `tcpiip-node-type` to the pool P2 and give the option the value `08af`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# option tcpiip-node-type 08af
```

To add multiple IP addresses for the ip-type option 175, use the command:

```
awplus(dhcp-config)# option 175 192.0.2.6
awplus(dhcp-config)# option 175 192.0.2.12
awplus(dhcp-config)# option 175 192.0.2.33
```

To add the option 179 to a pool, and give the option the value `123456`, use the command:

```
awplus(dhcp-config)# option 179 123456
```

To add a user-defined flag option with the name `perform-router-discovery`, use the command:

```
awplus(dhcp-config)# option perform-router-discovery yes
```

To clear all user-defined options from a DHCP address pool, use the command:

```
awplus(dhcp-config)# no option
```

To clear a user-defined option, named `tftp-server-name`, use the command:

```
awplus(dhcp-config)# no option tftp-server-name
```

**Related commands**

- [dns-server](#)
- [ip dhcp option](#)
- [lease](#)
- [service dhcp-server](#)
- [show ip dhcp pool](#)

# probe enable

**Overview** Use this command to enable lease probing for a DHCP pool. Probing is used by the DHCP server to check if an IP address it wants to lease to a client is already being used by another host.

The **no** variant of this command disables probing for a DHCP pool.

**Syntax** probe enable  
no probe enable

**Default** Probing is enabled by default.

**Mode** DHCP Pool Configuration

**Examples** To enable probing for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe enable
```

To disable probing for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe enable
```

**Related commands**

- ip dhcp pool
- probe packets
- probe timeout
- probe type
- show ip dhcp pool

# probe packets

**Overview** Use this command to specify the number of packets sent for each lease probe. Lease probing is configured on a per-DHCP pool basis. When set to 0 probing is effectively disabled.

The **no** variant of this command sets the number of probe packets sent to the default of 5.

**Syntax** `probe packets <0-10>`  
`no probe packets`

| Parameter | Description                       |
|-----------|-----------------------------------|
| <0-10>    | The number of probe packets sent. |

**Default** The default is 5.

**Mode** DHCP Pool Configuration

**Examples** To set the number of probe packets to 2 for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe packets 2
```

To set the number of probe packets to the default 5 for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe packets
```

**Related commands** [probe enable](#)  
[probe timeout](#)  
[probe type](#)  
[show ip dhcp pool](#)

# probe timeout

**Overview** Use this command to set the timeout value in milliseconds that the server waits for a response after each probe packet is sent. Lease probing is configured on a per-DHCP pool basis.

The **no** variant of this command sets the probe timeout value to the default setting, 200 milliseconds.

**Syntax** `probe timeout <50-5000>`  
`no probe timeout`

| Parameter                    | Description                       |
|------------------------------|-----------------------------------|
| <code>&lt;50-5000&gt;</code> | Timeout interval in milliseconds. |

**Default** The default timeout interval is 200 milliseconds.

**Mode** DHCP Pool Configuration

**Examples** To set the probe timeout value to 500 milliseconds for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe timeout 500
```

To set the probe timeout value for pool P2 to the default, 200 milliseconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe timeout
```

**Related commands** [probe enable](#)  
[probe packets](#)  
[probe type](#)  
[show ip dhcp pool](#)

# probe type

**Overview** Use this command to set the probe type for a DHCP pool. The probe type specifies how the DHCP server checks whether an IP address is being used by other hosts, referred to as lease probing. If **arp** is specified, the server sends an ARP request to determine if an address is in use. If **ping** is specified, the server will send an ICMP Echo Request (ping).

The **no** variant of this command sets the probe type to the default setting, ping.

**Syntax** probe type {arp|ping}  
no probe type

| Parameter | Description       |
|-----------|-------------------|
| arp       | Probe using ARP.  |
| ping      | Probe using ping. |

**Default** The default probe type is ping.

**Mode** DHCP Pool Configuration

**Examples** To set the probe type to arp for the pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe type arp
```

To set the probe type for the pool P2 to the default, ping, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe type
```

**Related commands**

- [ip dhcp pool](#)
- [probe enable](#)
- [probe packets](#)
- [probe timeout](#)
- [show ip dhcp pool](#)

# range

**Overview** This command adds an address range to the DHCP address pool you are configuring. The DHCP server responds to client requests received from the pool's network. It assigns an IP addresses within the specified range. The IP address range must lie within the network. You can add multiple address ranges and individual IP addresses for a DHCP pool by using this command multiple times.

The **no** variant of this command removes an address range from the DHCP pool. Use the **no range all** command to remove all address ranges from the DHCP pool.

**Syntax** `range <ip-address> [<ip-address>]`  
`no range <ip-address> [<ip-address>]`  
`no range all`

| Parameter                       | Description  |
|---------------------------------|--|
| <code>&lt;ip-address&gt;</code> | IPv4 address range for DHCP clients, in dotted decimal notation. The first IP address is the low end of the range, the second IP address is the high end. Specify only one IP address to add an individual IP address to the address pool. |

**Mode** DHCP Configuration

**Examples** To add an address range of 192.0.2.5 to 192.0.2.16 to the pool `Nerv_Office`, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# range 192.0.2.5 192.0.2.16
```

To add the individual IP address 192.0.2.2 to a pool, use the command:

```
awplus(dhcp-config)# range 192.0.2.2
```

To remove all address ranges from a pool, use the command:

```
awplus(dhcp-config)# no range all
```

**Related commands**

- `ip dhcp pool`
- `service dhcp-server`
- `show ip dhcp pool`

# route

**Overview** This command allows the DHCP server to provide static routes to clients.

**Syntax** `route A.B.C.D/M A.B.C.D {both|opt249|rfc3442}`

| Parameter | Description                            |
|-----------|--|
| A.B.C.D/M | Subnet for the route                   |
| A.B.C.D   | Next hop for the route                 |
| both      | opt249 and rfc3442                     |
| opt249    | Classless static route option for DHCP |
| rfc3442   | Classless static route option for DHCP |

**Mode** DHCP Configuration

**Examples** To distribute static routes for route 0.0.0.0/0 whose next hop is 192.16.1.1 to clients using both opt249 and rfc3442, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool public
awplus(dhcp-config)# route 0.0.0.0/0 192.16.1.1 both
```

**Related commands** [ip dhcp pool](#)



# service dhcp-relay

**Overview** This command enables the DHCP Relay Agent on the device. However, on a given IP interface, no DHCP forwarding takes place until at least one DHCP server is specified to forward/relay all clients' DHCP packets to.

The **no** variant of this command disables the DHCP Relay Agent on the device for all interfaces.

**Syntax** `service dhcp-relay`  
`no service dhcp-relay`

**Mode** Global Configuration

**Usage notes** A maximum number of 400 DHCP Relay Agents (one per interface) can be configured on the device. Once this limit has been reached, any further attempts to configure DHCP Relay Agents will not be successful.

**Default** The DHCP-relay service is enabled by default.

**Examples** To enable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
```

To disable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# no service dhcp-relay
```

**Related commands**

- [ip dhcp-relay agent-option](#)
- [ip dhcp-relay agent-option checking](#)
- [ip dhcp-relay information policy](#)
- [ip dhcp-relay maxhops](#)
- [ip dhcp-relay server-address](#)

# service dhcp-server

**Overview** This command enables the DHCP server on your device. The server then listens for DHCP requests on all IP interfaces. It will not run if there are no IP interfaces configured.

The **no** variant of this command disables the DHCP server.

**Syntax** `service dhcp-server`  
`no service dhcp-server`

**Mode** Global Configuration

**Example** To enable the DHCP server, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-server
```

**Related commands** [ip dhcp pool](#)  
[show ip dhcp server summary](#)  
[subnet-mask](#)

# short-lease-threshold

**Overview** Use this command to configure a short lease threshold.

Use the **no** variant of this command to return the short lease threshold to the default of one minute.

**Syntax** `short-lease-threshold <hours> <minutes>`  
`no short-lease-threshold`

| Parameter                    | Description                          |
|------------------------------|--------------------------------------|
| <code>&lt;hours&gt;</code>   | The number of hours, from 0 to 24.   |
| <code>&lt;minutes&gt;</code> | The number of minutes, from 0 to 60. |

**Default** 1 minute.

**Mode** DHCP Configuration

**Usage notes** DHCP leases need to be backed up in NVS so that when the DHCP server reboots or goes through a power cycle it won't lose all the knowledge of these leases.

Some networks have a high number of mobile devices repeatedly requesting DHCP leases every few seconds before their existing lease expires. This can happen for example, when mobile devices move in and out of a Wi-Fi zone or when Wi-Fi signal strength changes. This means the same IP address can have multiple lease entries which can take up unnecessary backup file space.

The **short-lease-threshold** command allows you to configure the threshold for a short lease, from 1 minute to 24 hours. Any lease less than the threshold is deemed to be a short lease and will NOT be backed up to NVS.

This is useful if you have:

- limited backup file space, and
- you don't need to restore leases after a device reboot or power cycle

**Example** To set the short lease threshold for address pool P2 to 40 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# short-lease-threshold 0 40
```

To set the short lease threshold for address pool Nerv\_Office to 5 hours and 35 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# short-lease-threshold 5 35
```

To return the short lease threshold to the default of one minute, use the following commands:

```
awplus# configure terminal
awplus(config)# no short-lease-threshold
```

**Related commands**

[lease](#)

**Command changes**

Version 5.4.8-2.1: command added

# show counter dhcp-client

**Overview** This command shows counters for the DHCP client on your device.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show counter dhcp-client

**Mode** User Exec and Privileged Exec

**Example** To display the message counters for the DHCP client on your device, use the command:

```
awplus# show counter dhcp-client
```

**Output** Figure 20-2: Example output from the **show counter dhcp-client** command

```
show counter dhcp-client
DHCPDISCOVER out      ..... 10
DHCPREQUEST out       ..... 34
DHCPCDECLINE out      ..... 4
DHCPRELEASE out       ..... 0
DHCPPOFFER in         ..... 22
DHCPACK in             ..... 18
DHCPNAK in            ..... 0
```

**Table 1:** Parameters in the output of the **show counter dhcp-client** command

| Parameter        | Description  |
|------------------|--|
| DHCPDISCOVER out | The number of DHCP Discover messages sent by the client.                     |
| DHCPREQUEST out  | The number of DHCP Request messages sent by the client.                      |
| DHCPCDECLINE out | The number of DHCP Decline messages sent by the client.                      |
| DHCPRELEASE out  | The number of DHCP Release messages sent by the client.                      |
| DHCPPOFFER in    | The number of DHCP Offer messages received by the client.                    |
| DHCPACK in       | The number of DHCP Acknowledgement messages received by the client.          |
| DHCPNAK in       | The number of DHCP Negative Acknowledgement messages received by the client. |

**Related commands** [ip address dhcp](#)

# show counter dhcp-relay

**Overview** This command shows counters for the DHCP Relay Agent on your device.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show counter dhcp-relay

**Mode** User Exec and Privileged Exec

**Examples** To display counters for the DHCP Relay Agent on your device, use the following command:

```
awplus# show counter dhcp-relay
```

**Output** Figure 20-3: Example output from the **show counter dhcp-relay** command

```
awplus#show counter dhcp-relay

DHCP relay counters
Requests In           ..... 4
Replies In           ..... 4
Relayed To Server    ..... 4
Relayed To Client    ..... 4
Out To Server Failed ..... 0
Out To Client Failed ..... 0
Invalid hlen         ..... 0
Bogus giaddr         ..... 0
Corrupt Agent Option ..... 0
Missing Agent Option ..... 0
Bad Circuit ID       ..... 0
Missing Circuit ID    ..... 0
Bad Remote ID        ..... 0
Missing Remote ID    ..... 0
Option Insert Failed ..... 0
DHCPv6 Requests In  ..... 0
DHCPv6 Replies In   ..... 0
DHCPv6 Relayed to Server ..... 0
DHCPv6 Relayed to Client ..... 0
```

| Parameter         | Description  |
|-------------------|--|
| Requests In       | The number of DHCP Request messages received from clients. |
| Replies In        | The number of DHCP Reply messages received from servers.   |
| Relayed To Server | The number of DHCP Request messages relayed to servers.    |
| Relayed To Client | The number of DHCP Reply messages relayed to clients.      |

| Parameter            | Description  |
|----------------------|--|
| Out To Server Failed | The number of failures when attempting to send request messages to servers. This is an internal debugging counter.   |
| Out To Client Failed | The number of failures when attempting to send reply messages to clients. This is an internal debugging counter.   |
| Invalid hlen         | The number of incoming messages dropped due to an invalid hlen field.  |
| Bogus giaddr         | The number of incoming DHCP Reply messages dropped due to the bogus giaddr field.  |
| Corrupt Agent Option | The number of incoming DHCP Reply messages dropped due to a corrupt relay agent information option field. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command. |
| Missing Agent Option | The number of incoming DHCP Reply messages dropped due to a missing relay agent information option field. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command. |
| Bad Circuit ID       | The number of incoming DHCP Reply messages dropped due to a bad circuit ID. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.                               |
| Missing Circuit ID   | The number of incoming DHCP Reply messages dropped due to a missing circuit ID. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.                           |

| Parameter                | Description  |
|--------------------------|--|
| Bad Remote ID            | The number of incoming DHCP Reply messages dropped due to a bad remote ID.<br>Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command  |
| Missing Remote ID        | The number of incoming DHCP Reply messages dropped due to a missing remote ID.<br>Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command  |
| Option Insert Failed     | The number of incoming DHCP Request messages dropped due to an error adding the DHCP Relay Agent information (option-82). This counter increments when: <ul style="list-style-type: none"> <li>the DHCP Relay Agent is set to drop packets with the DHCP Relay Agent Option 82 field already filled by another DHCP Relay Agent. This policy is set with the <code>ip dhcp-relay information policy</code> command.</li> <li>there is a packet error that stops the DHCP Relay Agent from being able to append the packet with its DHCP Relay Agent Information Option (Option 82) field.</li> </ul> |
| DHCPv6 Requests In       | The number of incoming DHCPv6 Request messages.  |
| DHCPv6 Replies In        | The number of incoming DHCPv6 Reply messages.  |
| DHCPv6 Relayed to Server | The number of DHCPv6 messages relayed to the server.   |
| DHCPv6 Relayed to Client | The number of DHCPv6 messages relayed to the client.   |



# show counter dhcp-server

**Overview** This command shows counters for the DHCP server on your device.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show counter dhcp-server`

**Mode** User Exec and Privileged Exec

**Example** To display counters for the DHCP server on your device, use the command:

```
awplus# show counter dhcp-server
```

**Output** Figure 20-4: Example output from the **show counter dhcp-server** command

|                      |       |    |
|----------------------|-------|----|
| DHCP server counters |       |    |
| DHCPDISCOVER in      | ..... | 20 |
| DHCPREQUEST in       | ..... | 12 |
| DHCPDECLINE in       | ..... | 1  |
| DHCPRELEASE in       | ..... | 0  |
| DHCPINFORM in        | ..... | 0  |
| DHCPOFFER out        | ..... | 8  |
| DHCPACK out          | ..... | 4  |
| DHCPNAK out          | ..... | 0  |
| BOOTREQUEST in       | ..... | 0  |
| BOOTREPLY out        | ..... | 0  |

**Table 2:** Parameters in the output of the **show counter dhcp-server** command

| Parameter       | Description   |
|-----------------|---|
| DHCPDISCOVER in | The number of Discover messages received by the DHCP server.    |
| DHCPREQUEST in  | The number of Request messages received by the DHCP server.     |
| DHCPDECLINE in  | The number of Decline messages received by the DHCP server.     |
| DHCPRELEASE in  | The number of Release messages received by the DHCP server.     |
| DHCPINFORM in   | The number of Inform messages received by the DHCP server.      |
| DHCPOFFER out   | The number of Offer messages sent by the DHCP server.           |
| DHCPACK out     | The number of Acknowledgement messages sent by the DHCP server. |

**Table 2:** Parameters in the output of the **show counter dhcp-server** command

| Parameter      | Description   |
|----------------|---|
| DHCPNAK out    | The number of Negative Acknowledgement messages sent by the DHCP server. The server sends these after receiving a request that it cannot fulfil because either there are no available IP addresses in the related address pool, or the request has come from a client that doesn't fit the network setting for an address pool. |
| BOOTREQUEST in | The number of bootp messages received by the DHCP server from bootp clients.  |
| BOOTREPLY out  | The number of bootp messages sent by the DHCP server to bootp clients.  |

**Related commands**

- service dhcp-server
- show ip dhcp binding
- show ip dhcp server statistics
- show ip dhcp pool

# show dhcp lease

**Overview** This command shows details about the leases that the DHCP client has acquired from a DHCP server for interfaces on the device.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the “Getting Started with AlliedWare\_Plus” Feature Overview and Configuration Guide.

**Syntax** `show dhcp lease [<interface>]`

| Parameter                      | Description                                       |
|--------------------------------|---|
| <code>&lt;interface&gt;</code> | Interface name to display DHCP lease details for. |

**Mode** User Exec and Privileged Exec

**Example** To show the current lease expiry times for all interfaces, use the command:

```
awplus# show dhcp lease
```

To show the current lease for vlan1, use the command:

```
awplus# show dhcp lease vlan1
```

**Output** Figure 20-5: Example output from the **show dhcp lease vlan1** command

```
Interface vlan1
-----
IP Address:                192.168.22.4
Expires:                   13 Mar 2017 20:10:19
Renew:                     13 Mar 2017 18:37:06
Rebind:                    13 Mar 2017 19:49:29
Server:
Options:
  subnet-mask              255.255.255.0
  routers                  19.18.2.100,12.16.2.17
  dhcp-lease-time          3600
  dhcp-message-type        5
  domain-name-servers      192.168.100.50,19.88.200.33
  dhcp-server-identifier   192.168.22.1
  domain-name               alliedtelesis.com
```

**Related commands** [ip address dhcp](#)

# show ip dhcp binding

**Overview** This command shows the lease bindings that the DHCP server has allocated clients.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip dhcp binding [<ip-address>|<address-pool>]`

| Parameter                         | Description  |
|-----------------------------------|--|
| <code>&lt;ip-address&gt;</code>   | IPv4 address of a leased IP address, in dotted decimal notation. This displays the lease information for the specified IP address. |
| <code>&lt;address-pool&gt;</code> | Name of an address pool. This displays the lease information for all clients within the address pool.                              |

**Mode** User Exec and Privileged Exec

**Examples** To display all leases for every client in all address pools, use the command:

```
awplus# show ip dhcp binding
```

To display the details for the leased IP address 172.16.2.16, use the command:

```
awplus# show ip dhcp binding 172.16.2.16
```

To display the leases from the address pool MyPool, use the command:

```
awplus# show ip dhcp binding MyPool
```

**Output** Figure 20-6: Example output from the **show ip dhcp binding** command

```
Pool 30_2_network Network 172.16.2.0/24
DHCP Client Entries
IP Address      ClientId                Type      Expiry
-----
172.16.2.100   0050.fc82.9ede          Dynamic   21 Sep 2007 19:02:58
172.16.2.101   000e.a6ae.7c14          Static    Infinite
172.16.2.102   000e.a6ae.7c4c          Static    Infinite
172.16.2.103   000e.a69a.ac91          Static    Infinite
172.16.2.104   00e0.189d.5e41          Static    Infinite
172.16.2.150   00e0.2b04.5800          Static    Infinite
172.16.2.167   4444.4400.35c3          Dynamic   21 Sep 2007 14:58:41
```

**Related commands**

- clear ip dhcp binding
- ip dhcp pool
- lease
- range
- service dhcp-server
- show ip dhcp pool

# show ip dhcp pool

**Overview** This command displays the configuration details and system usage of the DHCP address pools configured on the device.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip dhcp pool [<address-pool>]`

| Parameter      | Description  |
|----------------|--|
| <address-pool> | Name of a specific address pool. This displays the configuration of the specified address pool only. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip dhcp pool`

**Output** Figure 20-7: Example output from the **show ip dhcp pool** command

```
Pool p1 :
network: 192.168.1.0/24
address ranges:
  addr: 192.168.1.10 to 192.168.1.18
static host addresses:
  addr: 192.168.1.12      MAC addr: 1111.2222.3333
lease <days:hours:minutes:seconds> <1:0:0:0>
subnet mask: 255.255.255.0 (pool's network mask)
Probe:
  Status:      Enabled      [Enabled]
  Type:        ARP          [Ping]
  Packets:     2            [5]
  Timeout:    200 msec     [200]
Dynamic addresses:
  Total:       8
  Leased:      2
  Utilization: 25.0 %
Static host addresses:
  Total:       1
  Leased:      1
```

Figure 20-8: Example output from the **show ip dhcp pool** command with IP address 192.168.1.12 assigned to a VLAN interface on the device:

```
Pool p1 :
network: 192.168.1.0/24
address ranges:
  addr: 192.168.1.10 to 192.168.1.18
        (interface addr 192.168.1.12 excluded)
        (static host addr 192.168.1.12 excluded)
static host addresses:
  addr: 192.168.1.12      MAC addr: 1111.2222.3333
        (= interface addr, so excluded)
lease <days:hours:minutes:seconds> <1:0:0:0>
subnet mask: 255.255.255.0 (pool's network mask)
Probe:                               Default Values
  Status:          Enabled             [Enabled]
  Type:            ARP                  [Ping]
  Packets:         2                    [5]
  Timeout:         200 msec             [200]
Dynamic addresses:
  Total:           8
  Leased:          2
  Utilization:    25.0 %
Static host addresses:
  Total:           1
  Leased:          1
```

Figure 20-9: Example output from the **show ip dhcp pool** command with a host with MAC 0000.cd38.05f9 is registered as a static host by DHCP Framed IP Lease feature from AUTHD:

```

Pool p1 :
  network: 10.1.1.0/24
  address ranges:
    addr: 10.1.1.101 to 10.1.1.199
          (static host addr 10.1.1.122 excluded)
          (static host addr 10.1.1.111 excluded)
  static host addresses:
    addr: 10.1.1.122      MAC addr: 0000.1111.2222
    addr: 10.1.1.111      MAC addr: 0000.cd38.05f9
                          Netmask : 255.255.255.0
                          Gateway  : 10.1.1.1
                          Lease   : 60 seconds
                          Added by AUTHD

  lease <1:0:0:0>
  subnet mask: 255.255.255.0 (pool's network mask)
  Probe:
    Status:      Enabled      [Enabled]
    Type:        Ping         [Ping]
    Packets:     5            [5]
    Timeout:     200 msec     [200]
  Dynamic addresses:
    Total:       97
    Leased:      1
    Utilization: 1.0 %
  Static host addresses:
    Total:       2
    Leased:      2
    
```

**Table 3:** Parameters in the output of the **show ip dhcp pool** command

| Parameter      | Description   |
|----------------|---|
| Pool           | Name of the pool.   |
| network        | Subnet and mask length of the pool.   |
| address ranges | Individual IP addresses and address ranges configured for the pool. The DHCP server can offer clients an IP address from within the specified ranges only.<br>Any of these addresses that match an interface address on the device, or a static host address configured in the pool, will be automatically excluded from the range, and a message to this effect will appear beneath the range entry. |



**Table 3:** Parameters in the output of the **show ip dhcp pool** command (cont.)

| Parameter                       | Description   |
|---------------------------------|---|
| static host addresses           | The static host addresses configured on the pool. Each IP address is permanently assigned to the client with the matching MAC address. Any of these addresses that match an interface address on the device will be automatically excluded, and a message to this effect will appear beneath the static host entry. |
| lease <days:hours:minutes>      | The lease duration for address allocated by this pool.  |
| domain                          | The domain name sent by the pool to clients. This is the domain name that the client should use when resolving host names using DNS.  |
| subnet mask                     | The subnet mask sent by the pool to clients.  |
| Probe - Status                  | Whether lease probing is enabled or disabled.   |
| Probe - Type                    | The lease probe type configured. Either ping or ARP.  |
| Probe - Packets                 | The number of packets sent for each lease probe in the range 0 to 10.   |
| Probe - Timeout                 | The timeout value in milliseconds to wait for a response after each probe packet is sent. In the range 50 to 5000.  |
| dns servers                     | The DNS server addresses sent to by the pool to clients.  |
| default-router(s)               | The default router addresses sent by the pool to clients.   |
| user-defined options            | The list of user-defined options sent by the pool to clients.   |
| Dynamic addresses- Total        | The total number of IP addresses that have been configured in the pool for dynamic allocation to DHCP clients.  |
| Dynamic addresses- Leased       | The number of IP addresses in the pool that have been dynamically allocated (leased) to DHCP clients.   |
| Dynamic addresses - Utilization | The percentage of IP addresses in the pool that are currently dynamically allocated to clients.   |
| Static host addresses- Total    | The number of static IP addresses configured in the pool for specific DHCP client hosts.  |
| Static host addresses - Leased  | The number of static IP addresses assigned to specific DHCP client hosts.   |

**Related commands**

- ip dhcp pool
- probe enable
- probe packets
- probe timeout
- probe type
- range
- service dhcp-server
- subnet-mask

# show ip dhcp-relay

**Overview** This command shows the configuration of the DHCP Relay Agent on each interface.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip dhcp-relay [interface <interface-name>]`

| Parameter        | Description  |
|------------------|--|
| <interface-name> | Name of a specific interface. This displays the DHCP configuration for the specified interface only. |

**Mode** User Exec and Privileged Exec

**Example** To display the DHCP Relay Agent’s configuration on the interface vlan1, use the command:

```
awplus# show ip dhcp-relay interface vlan1
```

**Output** Figure 20-10: Example output from the **show ip dhcp-relay** command

```
DHCP Relay Service is enabled

vlan1 is up, line protocol is up
Maximum hop count is 10
Insertion of Relay Agent Option is disabled
Checking of Relay Agent Option is disabled
The Remote Id string for Relay Agent Option is 0000.cd28.074c
Relay information policy is to append new relay agent
information
List of servers : 192.168.1.200
```

- Related commands**
- [ip dhcp-relay agent-option](#)
  - [ip dhcp-relay agent-option checking](#)
  - [ip dhcp-relay information policy](#)
  - [ip dhcp-relay maxhops](#)
  - [ip dhcp-relay server-address](#)

# show ip dhcp server statistics

**Overview** This command shows statistics related to the DHCP server.

You can display the server counters using the `show counter dhcp-server` command as well as with this command.

For information on filtering and saving command output, see the “Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide.

**Syntax** `show ip dhcp server statistics`

**Mode** User Exec and Privileged Exec

**Example** To display the server statistics, use the command:

```
awplus# show ip dhcp server statistics
```

**Output** Figure 20-11: Example output from the `show ip dhcp server statistics` command

```
DHCP server counters
DHCPDISCOVER in      ..... 20
DHCPREQUEST in       ..... 12
DHCPDECLINE in        ..... 1
DHCPRELEASE in        ..... 0
DHCPINFORM in         ..... 0
DHCPOFFER out         ..... 8
DHCPACK out           ..... 4
DHCPNAK out           ..... 0
BOOTREQUEST in        ..... 0
BOOTREPLY out         ..... 0
DHCPLEASEQUERY in     ..... 0
DHCPLEASEUNKNOWN out  ..... 0
DHCPLEASEACTIVE out   ..... 0
DHCPLEASEUNASSIGNED out ..... 0
```

**Table 4:** Parameters in the output of the `show ip dhcp server statistics` command

| Parameter       | Description  |
|-----------------|--|
| DHCPDISCOVER in | The number of Discover messages received by the DHCP server. |
| DHCPREQUEST in  | The number of Request messages received by the DHCP server.  |
| DHCPDECLINE in  | The number of Decline messages received by the DHCP server.  |

**Table 4:** Parameters in the output of the **show ip dhcp server statistics** command (cont.)

| Parameter               | Description   |
|-------------------------|---|
| DHCPRELEASE in          | The number of Release messages received by the DHCP server.   |
| DHCPINFORM in           | The number of Inform messages received by the DHCP server.  |
| DHCPOFFER out           | The number of Offer messages sent by the DHCP server.   |
| DHCPACK out             | The number of Acknowledgement messages sent by the DHCP server.   |
| DHCPNAK out             | The number of Negative Acknowledgement messages sent by the DHCP server. The server sends these after receiving a request that it cannot fulfil because either there are no available IP addresses in the related address pool, or the request has come from a client that doesn't fit the network setting for an address pool. |
| BOOTREQUEST in          | The number of bootp messages received by the DHCP server from bootp clients.  |
| BOOTREPLY out           | The number of bootp messages sent by the DHCP server to bootp clients.  |
| DHCPLEASEQUERY in       | The number of Lease Query messages received by the DHCP server from DHCP Relay Agents.  |
| DHCPLEASEUNKNOWN out    | The number of Lease Unknown messages sent by the DHCP server to DHCP Relay Agents.  |
| DHCPLEASEACTIVE out     | The number of Lease Active messages sent by the DHCP server to DHCP Relay Agents.   |
| DHCPLEASEUNASSIGNED out | The number of Lease Unassigned messages sent by the DHCP server to DHCP Relay Agents.   |

**Related commands**

- [show counter dhcp-server](#)
- [service dhcp-server](#)
- [show ip dhcp binding](#)
- [show ip dhcp pool](#)

# show ip dhcp server summary

**Overview** This command shows the current configuration of the DHCP server. This includes:

- whether the DHCP server is enabled
- whether the DHCP server is configured to ignore BOOTP requests
- whether the DHCP server is configured to support DHCP lease queries
- the details of any user-defined options
- a list of the names of all DHCP address pools currently configured

This show command does not include any configuration details of the address pools. You can display these using the [show ip dhcp pool](#) command.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip dhcp server summary`

**Mode** User Exec and Privileged Exec

**Example** To display the current configuration of the DHCP server, use the command:

```
awplus# show ip dhcp server summary
```

**Output** Figure 20-12: Example output from the **show ip dhcp server summary** command

```
DHCP Server service is disabled
BOOTP ignore is disabled
DHCP leasequery support is disabled
Pool list: p2
```

**Related commands**

- [ip dhcp leasequery enable](#)
- [ip dhcp pool](#)
- [service dhcp-server](#)

# subnet-mask

**Overview** This command sets the subnet mask option for a DHCP address pool you are configuring. Use this command to specify the client's subnet mask as defined in RFC 950. This sets the subnet details using the pre-defined option 1. Note that if you create a user-defined option 1 using the [option](#) command, then you will override any settings created with this command. If you do not specify a subnet mask using this command, then the pool's network mask (specified using the [next-server](#) command) is applied.

The **no** variant of this command removes a subnet mask option from a DHCP pool. The pool reverts to using the pool's network mask.

**Syntax** `subnet-mask <mask>`  
`no subnet-mask`

| Parameter                 | Description   |
|---------------------------|---|
| <code>&lt;mask&gt;</code> | Valid IPv4 subnet mask, in dotted decimal notation. |

**Mode** DHCP Configuration

**Examples** To set the subnet mask option to 255 . 255 . 255 . 0 for DHCP pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# subnet-mask 255.255.255.0
```

To remove the subnet mask option from DHCP pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no subnet-mask
```

**Related commands**

- [default-router](#)
- [dns-server](#)
- [domain-name](#)
- [next-server](#)
- [option](#)
- [service dhcp-server](#)
- [show ip dhcp pool](#)

# 21

# DHCP for IPv6 (DHCPv6) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure DHCPv6. For more information, see the [DHCPv6 Feature Overview and Configuration Guide](#).

DHCPv6 is a network protocol used to configure IPv6 hosts with IPv6 addresses and IPv6 prefixes for an IPv6 network. DHCPv6 is used instead of SLAAC (Stateless Address Autoconfiguration) at sites where centralized management of IPv6 hosts is needed. IPv6 routers require automatic configuration of IPv6 addresses and IPv6 prefixes.

DHCPv6 Prefix Delegation provides automatic configuration of IPv6 addresses and IPv6 prefixes.

Note that DHCPv6 client does not support tunnel interface.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**NOTE:** The IPv6 addresses shown use the address space 2001:0db8::/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical networks (other than for testing purposes) nor should they appear on any public network.

- Command List**
- [“address prefix”](#) on page 970
  - [“address range”](#) on page 972
  - [“clear counter ipv6 dhcp-client”](#) on page 974
  - [“clear counter ipv6 dhcp-server”](#) on page 975
  - [“clear ipv6 dhcp binding”](#) on page 976
  - [“clear ipv6 dhcp client”](#) on page 978
  - [“dns-server \(DHCPv6\)”](#) on page 979
  - [“domain-name \(DHCPv6\)”](#) on page 981



- [“ip dhcp-relay agent-option”](#) on page 982
- [“ip dhcp-relay agent-option checking”](#) on page 984
- [“ip dhcp-relay agent-option remote-id”](#) on page 986
- [“ip dhcp-relay information policy”](#) on page 988
- [“ip dhcp-relay maxhops”](#) on page 990
- [“ip dhcp-relay max-message-length”](#) on page 991
- [“ip dhcp-relay server-address”](#) on page 993
- [“ipv6 address \(DHCPv6 PD\)”](#) on page 995
- [“ipv6 address dhcp”](#) on page 998
- [“ipv6 dhcp client pd”](#) on page 1000
- [“ipv6 dhcp option”](#) on page 1002
- [“ipv6 dhcp pool”](#) on page 1004
- [“ipv6 dhcp server”](#) on page 1006
- [“ipv6 local pool”](#) on page 1007
- [“ipv6 nd prefix \(DHCPv6\)”](#) on page 1009
- [“link-address”](#) on page 1011
- [“option \(DHCPv6\)”](#) on page 1013
- [“prefix-delegation pool”](#) on page 1015
- [“service dhcp-relay”](#) on page 1017
- [“show counter dhcp-relay”](#) on page 1018
- [“show counter ipv6 dhcp-client”](#) on page 1021
- [“show counter ipv6 dhcp-server”](#) on page 1023
- [“show ip dhcp-relay”](#) on page 1025
- [“show ipv6 dhcp”](#) on page 1026
- [“show ipv6 dhcp binding”](#) on page 1027
- [“show ipv6 dhcp interface”](#) on page 1030
- [“show ipv6 dhcp pool”](#) on page 1032
- [“sntp-address”](#) on page 1034

# address prefix

**Overview** Use this command in DHCPv6 Configuration mode to specify an address prefix for address assignment with DHCPv6 server pool configuration.

Use the **no** variant of this command to remove the address prefix from the DHCPv6 server pool.

**Syntax** `address prefix <ipv6-prefix/prefix-length> [lifetime {<valid-time>|infinite} {<preferred-time>|infinite}]`  
`no address prefix <ipv6-prefix/prefix-length>`

| Parameter                                      | Description   |
|--|---|
| <code>&lt;ipv6-prefix/prefix-length&gt;</code> | Specify an IPv6 prefix and prefix length. The prefix length indicates the length of the IPv6 prefix assigned to the pool. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.   |
| <code>lifetime</code>                          | Specify a time period for the hosts to remember router advertisements (RAs). If you specify the optional lifetime parameter with this command then you must also specify a <i>valid-time</i> and a <i>preferred-time</i> value. See the Usage notes below this parameter table for a description of preferred and valid lifetimes and how these determine deprecated or invalid IPv6 addresses upon expiry. |
| <code>&lt;valid-time&gt;</code>                | Specify a valid lifetime in seconds in the range <5-315360000>. The default valid lifetime is 2592000 seconds.  |
| <code>infinite</code>                          | Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.   |
| <code>&lt;preferred-time&gt;</code>            | Specify a preferred lifetime in seconds in the range <5-315360000>. The default preferred lifetime is 604800 seconds.   |

**Mode** DHCPv6 Configuration

**Default** The default valid lifetime is 2592000 seconds and the default preferred lifetime is 604800 seconds.

**Usage notes** This command creates a pool of prefixes from which addresses are assigned to clients on request, and allocates a network prefix from which the DHCPv6 Server leases addresses. This command is an alternative to using a range set using the [address range](#) command.

The DHCPv6 Server selects an IPv6 address from the range available allocated by the IPv6 prefix, randomly generating the suffix of the IPv6 address, with the specified preferred and valid lifetime leases. Leased IPv6 address are found in the

DHCPv6 Server REPLY packet, which is located within the IANA (Identity Association for Non-temporary Addresses) IA address field in the **REPLY** message.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

**Examples** To add IPv6 address prefix 2001:0db8:1::/48 for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# address prefix 2001:0db8:1::/48
```

To remove a configured IPv6 address prefix for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# no address prefix 2001:0db8:1::/48
```

**Related commands** [address range](#)  
[ipv6 dhcp pool](#)

**Validation Commands** [show ipv6 dhcp binding](#)  
[show ipv6 dhcp pool](#)

# address range

**Overview** Use this command in DHCPv6 Configuration mode to specify an address range for address assignment with DHCPv6 server pool configuration.

Use the **no** variant of this command to remove an address range from the DHCPv6 server pool.

**Syntax** `address range <first-ipv6-address>  
<last-ipv6-address>[lifetime {<valid-time>|infinite}  
{<preferred-time>|infinite}]  
no address range <first-ipv6-address> <last-ipv6-address>`

| Parameter                               | Description  |
|---|--|
| <code>&lt;first-ipv6-address&gt;</code> | Specify the first IPv6 address of the IPv6 address range, in hexadecimal notation in the format <code>X:X::X:X</code> .  |
| <code>&lt;last-ipv6-address&gt;</code>  | Specify the last IPv6 address of the IPv6 address range, in hexadecimal notation in the format <code>X:X::X:X</code> .   |
| <code>lifetime</code>                   | Optional. Specify a time period for the hosts to remember router advertisements (RAs).<br>If you specify this parameter then you must also specify a <i>valid-time</i> and a <i>preferred-time</i> value.<br>See the Usage notes below this parameter table for a description of preferred and valid lifetimes and how these determine deprecated or invalid IPv6 addresses upon expiry. |
| <code>&lt;valid-time&gt;</code>         | Specify a valid lifetime in seconds in the range <code>&lt;5-31536000&gt;</code> .<br>The default valid lifetime is 2592000 seconds.   |
| <code>infinite</code>                   | Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.  |
| <code>&lt;preferred-time&gt;</code>     | Specify a preferred lifetime in seconds in the range <code>&lt;5-31536000&gt;</code> .<br>The default preferred lifetime is 604800 seconds.  |

**Default** The default valid lifetime is 2592000 seconds and the default preferred lifetime is 604800 seconds.

**Mode** DHCPv6 Configuration

**Usage** Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

**Examples** To add the IPv6 address range 2001:0db8:1::1 to 2001:0db8:1fff::1 for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# address range 2001:0db8:1::1
2001:0db8:1fff::1
```

To remove a configured IPv6 address range for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# no address range
```

**Related commands** [address prefix](#)  
[ipv6 dhcp pool](#)

**Validation Commands** [show ipv6 dhcp binding](#)  
[show ipv6 dhcp pool](#)

# clear counter ipv6 dhcp-client

**Overview** Use this command in Privileged Exec mode to clear DHCPv6 client counters.

**Syntax** `clear counter ipv6 dhcp-client`

**Mode** Privileged Exec

**Example** To clear DHCPv6 client counters, use the following command:

```
awplus# clear counter ipv6 dhcp-client
```

**Related commands** [show counter ipv6 dhcp-client](#)

# clear counter ipv6 dhcp-server

**Overview** Use this command in Privileged Exec mode to clear DHCPv6 server counters.

**Syntax** `clear counter ipv6 dhcp-server`

**Mode** Privileged Exec

**Example** To clear DHCPv6 server counters, use the following command:

```
awplus# clear counter ipv6 dhcp-server
```

**Related commands** [show counter ipv6 dhcp-server](#)

# clear ipv6 dhcp binding

**Overview** Use this command in Privileged Exec mode to clear either a specific lease binding or the lease bindings as specified by the command parameters. The command will only take effect on dynamically allocated bindings, not statically configured bindings. This command clears binding entries on the DHCPv6 server binding table.

**Syntax** `clear ipv6 dhcp binding {ipv6 <prefix>|duid <DUID>|all|pool <name>}`

| Parameter                        | Description  |
|----------------------------------|--|
| <code>ipv6 &lt;prefix&gt;</code> | Optional. Specify the IPv6 prefix of the DHCPv6 client, in hexadecimal notation in the format X:X::X:X.  |
| <code>duid &lt;DUID&gt;</code>   | Specify the DUID (DHCPv6 unique ID) of the DHCPv6 client.  |
| <code>all</code>                 | All DHCPv6 bindings.   |
| <code>pool &lt;name&gt;</code>   | Description used to identify DHCPv6 server address pool. Valid characters are any printable character. If the name contains spaces then you must enclose these in "quotation marks". |

**Mode** Privileged Exec

**Usage notes** A specific binding may be deleted by **ipv6** address or **duid** address, or several bindings may be deleted at once using **all** or **pool**.

Note that if you specify to clear the **ipv6** or **duid** address of what is actually a static DHCPv6 binding, an error message is displayed. If **all** or **pool** are specified and one or more static DHCPv6 bindings exist within those addresses, any dynamic entries within those addresses are cleared but any static entries are not cleared.

The `clear ipv6 dhcp binding` command is used as a server function. A binding table entry on the DHCPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding, all prefix lifetimes have expired, or when a user runs the `clear ipv6 dhcp binding` command.

If the **clear ipv6 dhcp binding** command is used with the optional IPv6 address parameter, only the binding for the specified client is deleted. If the **clear ipv6 dhcp binding** command is used without the optional IPv6 address parameter, then all automatic client bindings are deleted from the DHCPv6 bindings table.



**Example** To clear all dynamic DHCPv6 server binding entries, use the command:

```
awplus# clear ipv6 dhcp binding all
```

**Output** Figure 21-1: Example output from the **clear ipv6 dhcp binding all** command

```
awplus#clear ipv6 dhcp binding all
% Deleted 1 entries
```

**Related commands** [show ipv6 dhcp binding](#)

# clear ipv6 dhcp client

**Overview** Use this command in Privileged Exec mode to restart a DHCPv6 client on an interface.

**Syntax** `clear ipv6 dhcp client <interface>`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;interface&gt;</code> | Specify the interface name to restart a DHCPv6 client on. |

**Mode** Privileged Exec

**Example** To restart a DHCPv6 client on interface 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>]`

| Parameter                         | Description  |
|-----------------------------------|--|
| <code>&lt;ipv6-address&gt;</code> | Specify an IPv6 address of the DNS server, in hexadecimal notation in the format <code>x : x : : x : x</code> . This parameter is required when adding a DNS server to the DHCPv6 address pool. All DNS servers are removed from the DHCPv6 pool if you enter the <code>no dns-server</code> command without this parameter. |

**Mode** DHCPv6 Configuration

**Examples** To add the DNS server with the assigned IPv6 address `2001:0db8:3000:3000::32` to the DHCPv6 server pool named `P2`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# dns-server 2001:0db8:3000:3000::32
```

To remove the DNS server with the assigned IPv6 address `2001:0db8:3000:3000::32` from the DHCPv6 server pool named `P2`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no dns-server 2001:0db8:3000:3000::32
```

To remove all DNS servers from the DHCPv6 server pool named `P2`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no dns-server
```

**Related  
commands**    `ipv6 dhcp pool`  
                  `option (DHCPv6)`  
                  `show ipv6 dhcp pool`

# domain-name (DHCPv6)

**Overview** Use this command in DHCPv6 Configuration mode to add a domain name to the DHCPv6 server address pool you are configuring.

Use the **no** variant of this command to remove a domain name from the address pool.

**Syntax** `domain-name <domain-name>`  
`no domain-name`

| Parameter                        | Description  |
|----------------------------------|--|
| <code>&lt;domain-name&gt;</code> | Specify the domain name you wish to assign the DHCPv6 server address pool. Valid characters are printable characters. If the name contains spaces then you must enclose it in "quotation marks". |

**Mode** DHCPv6 Configuration

**Usage** This command specifies the domain name that a client should use when resolving host names using the Domain Name System, and sets the domain name details using the pre-defined option 15. Note that if you add a user-defined option 15 using the [option \(DHCPv6\)](#) command, then you will override any settings created with this command.

**Examples** To add the domain name `Engineering` to DHCPv6 server pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# domain-name Engineering
```

To remove the domain name `Engineering` from DHCPv6 server pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no domain-name Engineering
```

**Related commands**

- [dns-server \(DHCPv6\)](#)
- [option \(DHCPv6\)](#)
- [show ipv6 dhcp pool](#)

# ip dhcp-relay agent-option

**Overview** This command enables the DHCP Relay Agent to insert the DHCP Relay Agent Information Option (Option 82) into the client-request packets that it relays to its DHCP server. This allows the DHCP Relay Agent to pass on information to the server about the network location of the client device. The DHCP Relay Agent strips the DHCP Relay Agent Option 82 field out of the DHCP server's response, so that the DHCP client never sees this field.

When the DHCP Relay Agent appends its DHCP Relay Agent Option 82 data into the packet, it first overwrites any pad options present; then if necessary, it increases the packet length to accommodate the DHCP Relay Agent Option 82 data.

The **no** variant of this command stops the DHCP Relay Agent from appending the Option 82 field onto DHCP requests before forwarding it to the server.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**NOTE:** *The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands [ip dhcp-relay agent-option](#) and [ip dhcp-relay information policy](#) have been configured.*

**Syntax** `ip dhcp-relay agent-option`  
`no ip dhcp-relay agent-option`

**Default** DHCP Relay Agent Information Option (Option 82) insertion is disabled by default.

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** Use this command to alter the DHCP Relay Agent Option 82 setting when your device is the first hop for the DHCP client. To limit the maximum length of the packet, use the [ip dhcp-relay max-message-length](#) command.

**Examples** To make the DHCP Relay Agent listening on vlan1 append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the DHCP Relay Agent from appending the DHCP Relay Agent Option 82 field on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay agent-option
```

To make the relay agent listening on PPP interface ppp0 append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the relay agent from appending the DHCP Relay Agent Option 82 field on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip dhcp-relay agent-option
```

**Related commands**

- [ip dhcp-relay agent-option remote-id](#)
- [ip dhcp-relay information policy](#)
- [ip dhcp-relay max-message-length](#)
- [service dhcp-relay](#)

# ip dhcp-relay agent-option checking

**Overview** This command enables the DHCP Relay Agent to check DHCP Relay Agent Information Option (Option 82) information in response packets returned from DHCP servers. If the information does not match the information it has for its own client (downstream) interface then the DHCP Relay Agent drops the packet. Note that [ip dhcp-relay agent-option](#) must be configured.

The DHCP Relay Agent Option 82 field is included in relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled ([ip dhcp-relay agent-option](#)), and
- DHCP Relay Agent is enabled on the device ([service dhcp-relay](#))

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay agent-option checking`  
`no ip dhcp-relay agent-option checking`

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Examples** To make the DHCP Relay Agent listening on vlan1 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay agent-option
awplus(config-if)# ip dhcp-relay agent-option checking
```

To stop the DHCP Relay Agent on vlan1 from checking the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay agent-option checking
```

To make the relay agent listening on PPP interface ppp0 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip dhcp-relay agent-option
awplus(config-if)# ip dhcp-relay agent-option checking
```

To stop the relay agent from checking the DHCP Relay Agent Information Option (Option 82) field on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip dhcp-relay agent-option checking
```



**Related commands**

- ip dhcp-relay agent-option
- ip dhcp-relay agent-option remote-id
- ip dhcp-relay information policy
- service dhcp-relay

# ip dhcp-relay agent-option remote-id

**Overview** Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field the DHCP Relay Agent inserts into clients' request packets. The Remote ID identifies the device that is inserting the DHCP Relay Agent Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the device's MAC address.

Use the **no** variant of this command to return the Remote ID for an interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay agent-option remote-id <remote-id>`  
`no ip dhcp-relay agent-option remote-id`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;remote-id&gt;</code> | An alphanumeric (ASCII) string, 1 to 63 characters in length. Additional characters allowed are hyphen (-), underscore (_) and hash (#). Spaces are not allowed. |

**Default** The Remote ID is set to the device's MAC address by default.

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled ([ip dhcp-relay agent-option](#)), and
- DHCP Relay Agent is enabled on the device ([service dhcp-relay](#))

**Examples** To set the Remote ID to myid for client DHCP packets received on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay agent-option remote-id
```

To set the Remote ID to myid for client DHCP packets received on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0 timeslots all
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0 timeslots all
awplus(config-if)# no ip dhcp-relay agent-option remote-id
```

**Related commands**

- [ip dhcp-relay agent-option](#)
- [ip dhcp-relay agent-option checking](#)
- [show ip dhcp-relay](#)

# ip dhcp-relay information policy

**Overview** This command sets the policy for how the DHCP relay deals with packets arriving from the client that contain DHCP Relay Agent Option 82 information.

If the command **ip dhcp-relay agent-option** has not been configured, then this command has no effect at all - no alteration is made to Option 82 information in packets arriving from the client side.

However, if the command **ip dhcp-relay agent-option** has been configured, this command modifies how the DHCP relay service deals with cases where the packet arriving from the client side already contains DHCP Relay Agent Option 82 information.

This command sets the action that the DHCP relay should take when a received DHCP client request contains DHCP Relay Agent Option 82 information.

By default, the DHCP Relay Agent replaces any existing DHCP Relay Agent Option 82 field with its own DHCP Relay Agent field. This is equivalent to the functionality of the **replace** parameter.

The **no** variant of this command returns the policy to the default behavior - i.e. replacing the existing DHCP Relay Agent Option 82 field.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**NOTE:** The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands [ip dhcp-relay agent-option](#) and [ip dhcp-relay information policy](#) have been configured.

**Syntax** `ip dhcp-relay information policy {append|drop|keep|replace}`  
`no ip dhcp-relay information policy`

| Parameter | Description  |
|-----------|--|
| append    | The DHCP Relay Agent appends the DHCP Relay Agent Option 82 field of the packet with its own DHCP Relay Agent Option 82 details.                               |
| drop      | The DHCP Relay Agent discards the packet.  |
| keep      | The DHCP Relay Agent forwards the packet without altering the DHCP Relay Agent Option 82 field.  |
| replace   | The DHCP Relay Agent replaces the existing DHCP Relay Agent details in the DHCP Relay Agent Option 82 field with its own details before forwarding the packet. |

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Examples** To make the DHCP Relay Agent listening on vlan1 drop any client requests that already contain DHCP Relay Agent Option 82 information, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay information policy drop
```

To reset the DHCP relay information policy to the default policy for interface vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay information policy
```

**Related commands**

- [ip dhcp-relay agent-option](#)
- [ip dhcp-relay agent-option checking](#)
- [service dhcp-server](#)

# ip dhcp-relay maxhops

**Overview** This command sets the hop count threshold for discarding BOOTP messages. When the hops field in a BOOTP message exceeds the threshold, the DHCP Relay Agent discards the BOOTP message. The hop count threshold is set to 10 hops by default.

Use the **no** variant of this command to reset the hop count to the default.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay maxhops <1-255>`  
`no ip dhcp-relay maxhops`

| Parameter | Description                  |
|-----------|------------------------------|
| <1-255>   | The maximum hop count value. |

**Default** The default hop count threshold is 10 hops.

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Example** To set the maximum number of hops to 5 for packets received on interface vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay maxhops 5
```

**Related commands** [service dhcp-relay](#)

# ip dhcp-relay max-message-length

**Overview** This command applies when the device is acting as a DHCP Relay Agent and DHCP Relay Agent Option 82 insertion is enabled. It sets the maximum DHCP message length (in bytes) for the DHCP packet with its DHCP Relay Agent Option 82 data inserted. From this value it calculates the maximum packet size that it will accept at its input. Packets that arrive greater than this value will be dropped.

The **no** variant of this command sets the maximum message length to its default of 1400 bytes.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay max-message-length <548-1472>`  
`no ip dhcp-relay max-message-length`

| Parameter  | Description   |
|------------|---|
| <548-1472> | The maximum DHCP message length (this is the message header plus the inserted DHCP option fields in bytes). |

**Default** The default is 1400 bytes.

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** When a DHCP Relay Agent (that has DHCP Relay Agent Option 82 insertion enabled) receives a request packet from a DHCP client, it will append the DHCP Relay Agent Option 82 component data, and forward the packet to the DHCP server. The DHCP client will sometimes issue packets containing pad option fields that can be overwritten with Option 82 data.

Where there are insufficient pad option fields to contain all the DHCP Relay Agent Option 82 data, the DHCP Relay Agent will increase the packet size to accommodate the DHCP Relay Agent Option 82 data. If the new (increased) packet size exceeds that defined by the **maximum-message-length** parameter, then the DHCP Relay Agent will drop the packet.

**NOTE:** Before setting this command, you must first run the `ip dhcp-relay agent-option` command. This will allow the DHCP Relay Agent Option 82 fields to be appended.

**Example** To set the maximum DHCP message length to 1200 bytes for packets arriving in interface vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
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 vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay max-message-length
```

**Related commands** [service dhcp-relay](#)



# ip dhcp-relay server-address

**Overview** This command adds a DHCP server for the DHCP Relay Agent to forward client DHCP packets to on a particular interface. You can add up to five DHCP servers on each device interface that the DHCP Relay Agent is listening on.

The **no** variant of this command deletes the specified DHCP server from the list of servers available to the DHCP relay agent.

The **no ip dhcp-relay** command removes all DHCP relay settings from the interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax**

```
ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}

no ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}

no ip dhcp-relay
```

| Parameter          | Description   |
|--------------------|---|
| <ipv4-address>     | Specify the IPv4 address of the DHCP server for the DHCP Relay Agent to forward client DHCP packets to, in dotted decimal notation. The IPv4 address uses the format A.B.C.D. |
| <ipv6-address>     | Specify the IPv6 address of the DHCPv6 server for the DHCPv6 Relay Agent to forward client DHCP packets to, in hexadecimal notation.  |
| <server-interface> | Specify the interface name of the DHCPv6 server. It is only required for a DHCPv6 server with an IPv6 address.  |

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** For a DHCP server with an IPv6 address you must specify the interface for the DHCP server. See examples below for configuration differences between IPv4 and IPv6 DHCP relay servers.

See also the [service dhcp-relay](#) command to enable the DHCP Relay Agent on your device. The [ip dhcp-relay server-address](#) command defines a relay destination on an interface on the device, needed by the DHCP Relay Agent to relay DHCP client packets to a DHCP server.

**Examples** To enable the DHCP Relay Agent to relay DHCP packets on interface vlan1 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 vlan1
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 vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay server-address 192.0.2.200
```

To disable DHCP relay on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay
```

**Related commands** [service dhcp-relay](#)

# 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                                    | Description  |
|--|--|
| <code>&lt;ipv6-prefix-name&gt;</code>        | The IPv6 prefix name advertised on the router advertisement message sent from the device. The IPv6 prefix name is delegated from the DHCPv6 Server configured for DHCPv6 Prefix-Delegation.      |
| <code>&lt;ipv6-addr/prefix-length&gt;</code> | Specifies the IPv6 address to be set, for example <code>::1/64</code> . The IPv6 address uses the format <code>X:X:X:X/Prefix-Length</code> . The prefix-length is usually set between 0 and 64. |
| <code>[eui64]</code>                         | EUI-64 is a method of automatically deriving the lower 64 bits of an IPv6 address, based on the switch's MAC address.  |

**Mode** Interface Configuration for a VLAN or a PPP interface.

**Usage notes** When specifying the **eui64** parameter, the interface identifier of the IPv6 address is derived from the MAC address of the device.

For more information about EUI64, see the [IPv6 Feature Overview and Configuration Guide](#).

**Examples** To configure a PD prefix named `prefix1` on interface `vlan1` and then add an IPv6 address, use the following commands. In this example, the prefix will be assigned from the pool on the PD client. The host portion or suffix will be `::1` for the last 64 bits:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd prefix1
awplus(config-if)# ipv6 address prefix1::1/64
```

To configure a PD prefix named `prefix1` on interface `vlan1` and then add an IPv6 address using EUI-64 identifiers, use the following commands. 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:

```
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
```

To assign the IPv6 address `2001:0db8::a2/48` to the VLAN interface `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 address 2001:0db8::a2/48
```

To remove the IPv6 address `2001:0db8::a2/48` from the VLAN interface `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
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 `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 address 2001:0db8::/64 eui64
```

To remove the **eui64** derived address in the prefix `2001:db8::/32` from VLAN interface `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
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

# ipv6 address dhcp

**Overview** Use this command to activate the DHCPv6 client on the interface that you are configuring. This allows the interface to use the DHCPv6 client to obtain its IPv6 configuration details from a DHCPv6 server on its connected network.

The command also enables IPv6 on the interface, which creates an EUI-64 link-local address as well as enabling RA processing and SLAAC.

Use the **no** variant of this command to stop the interface from obtaining IPv6 configuration details from a DHCPv6 server.

The DHCPv6 client supports the following IP configuration options:

- Option 1 - the subnet mask for your device.
- Option 3 - a list of default routers.
- Option 6 - a list of DNS servers. This list appends the DNS servers set on your device with the [dns-server \(DHCPv6\)](#) command.
- Option 15 - a domain name used to resolve host names. This option replaces any domain name that you have set with the [domain-name \(DHCPv6\)](#) command.
- Option 51 - lease expiration time.

**Syntax** `ipv6 address dhcp [default-route-to-server]`  
`no ipv6 address dhcp`

**Mode** Interface Configuration for a VLAN interface, a local loopback interface, or a PPP interface.

**Usage notes** Use the **default-route-to-server** option to allow the automatic configuration of a default route to the DHCPv6 server. Note that this option is not enabled by default when you enable the DHCP client on an interface.

**Examples** To set the interface `vlan1` to use DHCPv6 to obtain an IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 address dhcp
```

To stop the interface `vlan1` from using DHCPv6 to obtain its IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
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**

[clear ipv6 dhcp client](#)  
[ipv6 address](#)  
[ipv6 address \(DHCPv6 PD\)](#)  
[show ipv6 dhcp interface](#)  
[show running-config](#)

# ipv6 dhcp client pd

**Overview** Use this command in Interface Configuration mode to enable the DHCPv6 client process and enable requests for prefix delegation through the interface that you are configuring.

Use the **no** variant of this command to disable requests for prefix delegation. This is the default setting.

For further information about DHCPv6 Prefix Delegation, which is used to automate the process of assigning prefixes, see the [DHCPv6 Feature Overview and Configuration Guide](#).

**Syntax** `ipv6 dhcp client pd <prefix-name> <default-route-to-server>`  
`no ipv6 dhcp client pd`

| Parameter                                    | Description   |
|--|---|
| <code>&lt;prefix-name&gt;</code>             | Specify an IPv6 general prefix name. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks". |
| <code>&lt;default-route-to-server&gt;</code> | Specify the default route to the DHCP server  |

**Mode** Interface Configuration

**Default** Prefix delegation is disabled by default on an interface.

**Usage notes** Entering the **ipv6 dhcp client pd** command starts the DHCPv6 client process if not already running, and enables requests for prefix delegation through the interface on which the command is configured.

When prefix delegation is enabled and a prefix is acquired, the prefix is stored in the IPv6 prefix pool with an internal name defined by the required `<prefix-name>` placeholder parameter. The [ipv6 address](#) command can then refer to the prefixes stored in the IPv6 prefix pool.

**Examples** To enable prefix delegation with the prefix name `prefix-name` on the VLAN interface `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd my-prefix-name
```



To disable prefix delegation on the VLAN interface vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 dhcp client pd
```

**Related  
commands**

- [ipv6 enable](#)
- [clear ipv6 dhcp client](#)
- [ipv6 address \(DHCPv6 PD\)](#)
- [ipv6 nd prefix \(DHCPv6\)](#)
- [show ipv6 dhcp binding](#)
- [show ipv6 dhcp interface](#)

# ipv6 dhcp option

**Overview** Use this command in Global Configuration mode to create a user-defined DHCPv6 option. You can then use this option when configuring a DHCPv6 server address pool, by using the [option \(DHCPv6\)](#) command.

Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

Use the **no** variant of this command to remove either the specified user-defined option. This also removes user-defined options from the associated DHCPv6 server address pools.

**Syntax** `ipv6 dhcp option <1-254> [name <option-name>] [<option-type>]`  
`no ipv6 dhcp option <1-254> |<option-name>`

| Parameter     | Description   |       |                      |     |   |      |  |         |                                |      |   |
|---------------|---|-------|----------------------|-----|---|------|--|---------|--------------------------------|------|---|
| <1-254>       | The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.  |       |                      |     |   |      |  |         |                                |      |   |
| <option-name> | Option name used to identify the option. You cannot use a number as the option name. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".<br>Default: no default  |       |                      |     |   |      |  |         |                                |      |   |
| <option-type> | The option value. You must specify a value that is appropriate to the option type: <table border="1"><tbody><tr><td>ascii</td><td>An ASCII text string</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>ipv6</td><td>An IPv6 address or prefix that has hexadecimal notation in the format HHHH : HHHH : : HHHH : HHHH. To create a list of IPv6 addresses, you must add each IPv6 address individually by using the option command multiple times.</td></tr><tr><td>integer</td><td>A number from 0 to 4294967295.</td></tr><tr><td>flag</td><td>A value that either sets (to 1) or unsets (to 0) a flag: <b>true</b>, <b>on</b>, or <b>enabled</b> will set the flag. <b>false</b>, <b>off</b> or <b>disabled</b> will unset the flag.</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. | ipv6 | An IPv6 address or prefix that has hexadecimal notation in the format HHHH : HHHH : : HHHH : HHHH. To create a list of IPv6 addresses, you must add each IPv6 address individually by using the option command multiple times. | integer | A number from 0 to 4294967295. | flag | A value that either sets (to 1) or unsets (to 0) a flag: <b>true</b> , <b>on</b> , or <b>enabled</b> will set the flag. <b>false</b> , <b>off</b> or <b>disabled</b> will unset the flag. |
| ascii         | An ASCII text string  |       |                      |     |   |      |  |         |                                |      |   |
| hex           | A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.   |       |                      |     |   |      |  |         |                                |      |   |
| ipv6          | An IPv6 address or prefix that has hexadecimal notation in the format HHHH : HHHH : : HHHH : HHHH. To create a list of IPv6 addresses, you must add each IPv6 address individually by using the option command multiple times.  |       |                      |     |   |      |  |         |                                |      |   |
| integer       | A number from 0 to 4294967295.  |       |                      |     |   |      |  |         |                                |      |   |
| flag          | A value that either sets (to 1) or unsets (to 0) a flag: <b>true</b> , <b>on</b> , or <b>enabled</b> will set the flag. <b>false</b> , <b>off</b> or <b>disabled</b> will unset the flag.   |       |                      |     |   |      |  |         |                                |      |   |

**Mode** Global Configuration

**Examples** To define a user-defined ASCII string option as option 66, without a name, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 66 ascii
```

To define a user-defined hexadecimal string option as option 46, with the name "tcpip-node-type", use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 46 name tcpip-node-type hex
```

To define a user-defined IP address option as option 175, with the name special-address, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 175 name special-address ip
```

To remove the specific user-defined option with the option number 12, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp option 12
```

To remove the specific user-defined option with the option name perform-router-discovery, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp option perform-router-discovery
```

**Related commands**

[dns-server \(DHCPv6\)](#)  
[domain-name \(DHCPv6\)](#)  
[option \(DHCPv6\)](#)  
[show ipv6 dhcp](#)

# ipv6 dhcp pool

**Overview** Use this command in Global Configuration mode to enter the DHCPv6 Configuration mode for the DHCPv6 server pool name as specified in the required command parameter. If the name specified is not associated with an existing pool, the device will create a new pool with this name, then enter the configuration mode for the new pool.

Once you have entered the DHCPv6 configuration mode, all commands executed before the next **exit** command will apply to this pool.

You can create multiple DHCPv6 server pools on devices with multiple interfaces. This allows the device to act as a DHCPv6 server on multiple interfaces to distribute different information to clients on the different networks.

Use the **no** variant of this command to delete the specific DHCPv6 pool.

**Syntax** `ipv6 dhcp pool <DHCPv6-poolname>`  
`no ipv6 dhcp pool <DHCPv6-poolname>`

| Parameter                            | Description  |
|--------------------------------------|--|
| <code>&lt;DHCPv6-poolname&gt;</code> | Description used to identify this DHCPv6 server pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks". |

**Mode** Global Configuration

**Usage** All DHCPv6 prefix pool names must be unique. IPv6 prefix pools have a similar function to IPv4 address pools. Contrary to IPv4, a block of IPv6 addresses (an IPv6 address prefix) are assigned and not single IPv6 addresses. IPv6 prefix pools are not allowed to overlap.

Once a pool is configured, it cannot be changed. To change the configuration, you must remove then recreate a IPv6 prefix pool. All IPv6 prefixes already allocated are also freed.

**Examples** To create the DHCPv6 pool named P2 and enter DHCPv6 configuration mode, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)#
```

To delete the DHCPv6 pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp pool P2
```

**Related commands**

- ipv6 local pool
- option (DHCPv6)
- prefix-delegation pool
- show ipv6 dhcp binding
- show ipv6 dhcp pool

# ipv6 dhcp server

**Overview** Use this command in Interface Configuration mode to enable DHCPv6 server for the current IPv6 configured interface to use the specified DHCPv6 server pool name.

The DHCPv6 server service listens for DHCPv6 requests on the IPv6 configured interface. The DHCPv6 server service does not run on interfaces without IPv6 configured on them.

Use the **no** variant of this command to disable the DHCPv6 server.

**Syntax** `ipv6 dhcp-server [<DHCPv6-poolname>]`  
`no ipv6 dhcp-server`

| Parameter         | Description  |
|-------------------|--|
| <DHCPv6-poolname> | Specify a named DHCPv6 server pool as defined with the <code>ipv6 dhcp pool</code> command. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks". |

**Mode** Interface Configuration

**Usage notes** The **ipv6 dhcp server** command enables the DHCPv6 service on a specified interface using the pool for prefix delegation and configuration through the specified interface.

Note that DHCPv6 client, DHCPv6 server and DHCPv6 relay are mutually exclusive on an interface. When one of the DHCPv6 functions is enabled on an interface then another DHCPv6 function cannot be enabled on the same interface.

**Examples** To enable the DHCPv6 server service and use the DHCPv6 pool named P2 on VLAN interface vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 dhcp server P2
```

To disable the DHCPv6 server on VLAN interface vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 dhcp server
```

**Related commands** [ipv6 dhcp pool](#)  
[show ipv6 dhcp binding](#)  
[show ipv6 dhcp pool](#)

# ipv6 local pool

**Overview** Use this command in Global Configuration mode to configure a local DHCPv6 server prefix delegation pool specifying a poolname and a prefix/prefix length. You can optionally exclude the locally assigned prefix from the pool with the **exclude-local-prefix** keyword.

Use the **no** variant of this command to remove a local DHCPv6 server prefix delegation pool specifying the poolname.

**Syntax** `ipv6 local pool <DHCPv6-poolname> <delegated-prefix-name>  
<ipv6-prefix/prefix-length> <assigned-length>  
[exclude-local-prefix]`  
`no ipv6 local pool`

| Parameter                                      | Description  |
|--|--|
| <code>&lt;DHCPv6-poolname&gt;</code>           | Description used to identify this DHCPv6 server pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".   |
| <code>&lt;delegated-prefix-name&gt;</code>     | Description used to identify the delegated prefix name from the parent PD (Prefix Delegation) server. If the name contains spaces then you must enclose it in "quotation marks".   |
| <code>&lt;ipv6-prefix/prefix-length&gt;</code> | Specify an IPv6 prefix and prefix length. The prefix length indicates the length of the IPv6 prefix assigned to the pool.<br>The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.   |
| <code>&lt;assigned-length&gt;</code>           | Specify an IPv6 prefix length assigned to the user from the pool in the range <1-128>. Note that the value of the <i>assigned-length</i> parameter entered cannot be less than or equal to the <i>prefix-length</i> parameter value entered. An assigned length must be longer than a prefix length. |
| <code>exclude-local-prefix</code>              | Specify this keyword to exclude the locally assigned prefix from the pool.   |

**Default** No DHCPv6 server prefix delegation pool is configured by default.

**Mode** Global Configuration

**Usage notes** All IPv6 prefix pool names must be unique. IPv6 prefix pools have a similar function to IPv4 address pools. Contrary to IPv4, a block of IPv6 addresses (an IPv6 address prefix) are assigned and not single IPv6 addresses. IPv6 prefix pools are not allowed to overlap.

Once a pool is configured, it cannot be changed. To change the configuration, you must remove then recreate a IPv6 prefix pool. All IPv6 prefixes already allocated are also freed.

**Examples** To create a local DHCPv6 local pool named P2 with the IPv6 prefix and prefix length 2001:0db8::/32 with an assigned length of 64, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 local pool P2 2001:0db8::/32 64
```

To remove a configured DHCPv6 local pool, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 local pool
```

**Related commands** [ipv6 dhcp pool](#)  
[show ipv6 dhcp pool](#)



# ipv6 nd prefix (DHCPv6)

**Overview** Use this command to specify IPv6 RA (Router Advertisement) prefix information generated from the DHCPv6 server for DHCPv6 prefix-delegation for 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}`

| Parameter                               | Description  |
|---|--|
| <code>&lt;ipv6-prefix-name&gt;</code>   | The IPv6 prefix name advertised on the router advertisement message sent from the device.<br>The IPv6 prefix name is delegated from the DHCPv6 Server configured for DHCPv6 Prefix-Delegation.   |
| <code>&lt;ipv6-prefix/length&gt;</code> | The IPv6 prefix and prefix length advertised on the router advertisement message sent from the device.<br>The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.  |
| <code>&lt;valid-lifetime&gt;</code>     | The the period during which the specified IPv6 address prefix is valid. This can be set to a value between 5 and 315360000 seconds. Note that this period should be set to a value greater than that set for the prefix preferred-lifetime. See the Usage notes after this parameter table for a description of valid lifetime and how it determines invalid IPv6 addresses upon expiry.   |
| <code>infinite</code>                   | Specifying this keyword instead of entering a value for the <code>&lt;valid-lifetime&gt;</code> parameter applies an infinite valid lifetime.  |
| <code>&lt;preferred-lifetime&gt;</code> | Specifies the IPv6 prefix preferred lifetime. This is the period during which the IPv6 address prefix is considered current. Set this to a value between 0 and 315360000 seconds. Note that this period should be set to a value less than that set for the prefix valid-lifetime. See the Usage notes after this parameter table for a description of preferred lifetime and how it determines deprecated IPv6 addresses upon expiry. |
| <code>infinite</code>                   | Specifying this keyword instead of entering a value for the <code>&lt;preferred-lifetime&gt;</code> parameter applies an infinite valid lifetime.  |
| <code>off-link</code>                   | Specify the IPv6 prefix off-link flag.   |
| <code>no-autoconfig</code>              | Specify the IPv6 prefix no autoconfiguration flag. Setting this flag indicates that the prefix is not to be used for autoconfiguration.  |
| <code>all</code>                        | Specify all prefix names and all prefixes are removed when used with the no variant of this command.   |

**Mode** Interface Configuration for a VLAN interface or a PPP interface.

**Usage notes** This command specifies the IPv6 prefix flags that are advertised by the router advertisement message.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

**Examples** The following example configures the device to issue RAs (Router Advertisements) on the VLAN interface `vlan1`, and advertises the DHCPv6 prefix name `prefix1` and the IPv6 address prefix of `2001:0db8::/32`.

```
awplus# configure terminal
awplus(config)# interface vlan1
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 `vlan1`, so the address prefix of `2001:0db8::/32` is not advertised from the device.

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/32
```

The following example removes all prefix names and prefixes from VLAN interface `vlan1`:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 nd prefix all
```

**Related commands** [ipv6 address \(DHCPv6 PD\)](#)  
[ipv6 dhcp client pd](#)

[ipv6 dhcp pool](#)

[ipv6 local pool](#)

[prefix-delegation pool](#)

[show ipv6 dhcp binding](#)

# link-address

**Overview** Use this command in DHCPv6 Configuration mode to specify a link-address prefix within a DHCPv6 Server pool.

Note that you can only configure one link address per DHCPv6 pool. Configuring another link address in the same DHCPv6 pool overwrites the previously configured link address.

Use the **no** variant of this command to remove the link-address prefix from the DHCPv6 Server pool.

**Syntax** `link-address <ipv6-prefix/prefix-length>`  
`no link-address`

| Parameter                                      | Description   |
|--|---|
| <code>&lt;ipv6-prefix/prefix-length&gt;</code> | Specify an IPv6 prefix and prefix length. The prefix length indicates the length of the IPv6 prefix assigned to the pool. The IPv6 address uses the format X:X::X/X/Prefix-Length. The prefix-length is usually set between 0 and 64. |

**Default** No DHCPv6 Server pool configuration link address prefix is configured by default.

**Mode** DHCPv6 Configuration

**Usage notes** Link addresses are configured in DHCPv6 Server address pools when there are remote clients that communicate via intermediate relay(s).

RELAY-FORW and RELAY-REPL relay packets contain the requesting link address source.

This command is used to match incoming requests from PD (Prefix Delegation) clients (received via an intermediate relay) to a configured delegation pool.

When an address on the incoming interface of the DHCPv6 server or a link address set in the incoming delegation request packet from the prefix delegation client matches the link-address prefix configured in the delegation pool, the DHCPv6 server is able to match and use the appropriate delegation pool for relayed delegation request messages.

If there is no match between incoming delegation request packets from the prefix delegation client and the link-address prefix configured in the delegation pool, the DHCPv6 Server does not delegate an IPv6 prefix to the requesting device.

The link address should be set to the network prefix where the prefix delegation client resides. The prefix delegation server will also need a forwarding path (IPv6 route) back to the network prefix where the prefix delegation client resides.

For more information, see the [DHCPv6 Feature Overview and Configuration Guide](#).

**Examples** To configure the IPv6 prefix and prefix length 2001:0db8:1::/48 as the link address for pool P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# address prefix 2001:0db8:2::/48
awplus(config-dhcp6)# link-address 2001:0db8:1::/48
```

To remove the link address, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# no link-address
```

**Related commands** [ipv6 dhcp pool](#)  
[show ipv6 dhcp pool](#)

# option (DHCPv6)

**Overview** Use this command in DHCPv6 Configuration mode to add a user-defined option to the DHCPv6 prefix pool you are configuring. For the **hex**, **integer**, and **flag** option types, if the option already exists, the new option overwrites the existing option's value.

Use the **no** variant of this command to remove the specified user-defined option from the DHCPv6 server pool, or to remove all user-defined options from the DHCPv6 server pool.

**Syntax** `option [<1-254>|<option-name>] <option-value>`  
`no option [<1-254>|<option-value>]`

| Parameter      | Description  |   |
|----------------|--|---|
| <1-254>        | The option number of the option. Options with the same number as one of the standard options overrides the standard option definition. |   |
| <option-name>  | Option name associated with the option.  |   |
| <option-value> | The option value. You must specify a value that is appropriate to the option type:   |   |
|                | hex  | A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long. |
|                | ipv6   | An IPv6 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.          |
|                | integer  | A number from 0 to 4294967295.  |
|                | flag   | A value of either true, on, or enabled to set the flag, or false, off or disabled to unset the flag.  |

**Mode** DHCPv6 Configuration

**Usage** You must define a DHCPv6 option using the `ipv6 dhcp option` command before using the `option (DHCPv6)` command.

Note that options with an **ipv6** type can hold a list of IPv6 prefix (i.e. entries that have the X : X : : X : X address format), so if the option already exists in the pool, then the new IP address is added to the list of existing IPv6 prefixes. Also note options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

**Examples** To add the IPv6 type option named `sntp-server-addr` to the pool P2 and give the option the value `ipv6`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 22 name sntp_server_addr ipv6
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option sntp_server_addr ipv6
```

To add the ASCII-type option named `tftp-server-name` to the pool P2 and give the option the value `server1`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option tftp-server-name server1
```

To add the hex-type option named `tcPIP-node-type` to the pool P2 and give the option the value `08af`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option tcPIP-node-type 08af
```

To add multiple IP addresses for the ip-type option 175, use the following commands:

```
awplus(config-dhcp6)# option 175 2001:0db8:3001::/64
awplus(config-dhcp6)# option 175 2001:0db8:3002::/64
awplus(config-dhcp6)# option 175 2001:0db8:3003::/64
```

To add the option 179 to a pool, and give the option the value `123456`, use the following command:

```
awplus(config-dhcp6)# option 179 123456
```

To add a user-defined flag option with the name `perform-router-discovery`, use the following command:

```
awplus(config-dhcp6)# option perform-router-discovery yes
```

To clear all user-defined options from a DHCP address pool, use the following command:

```
awplus(config-dhcp6)# no option
```

To clear a user-defined option, named `tftp-server-name`, use the following command:

```
awplus(config-dhcp6)# no option tftp-server-name
```

**Related commands**

- [dns-server \(DHCPv6\)](#)
- [ipv6 dhcp option](#)
- [ipv6 dhcp pool](#)
- [show ipv6 dhcp pool](#)

# prefix-delegation pool

**Overview** Use this command in DHCPv6 Configuration mode to add a DHCPv6 server prefix-delegation pool entry to the current DHCPv6 pool configuration. You must define a DHCPv6 server prefix-delegation pool using the `ipv6 dhcp pool` command before using this command.

Use the **no** variant of this command to remove a DHCPv6 server prefix-delegation pool from the current DHCPv6 pool configuration.

**Syntax** `prefix-delegation pool <DHCPv6-poolname> [lifetime {<valid-time>|infinite} {<preferred-time>|infinite}]`  
`no prefix-delegation pool <DHCPv6-poolname>`

| Parameter                            | Description   |
|--------------------------------------|---|
| <code>&lt;DHCPv6-poolname&gt;</code> | Description used to identify this DHCPv6 server pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".  |
| <code>lifetime</code>                | Optional. Specify a time period for the hosts to remember router advertisements (RAs). If you specify this parameter then you must also specify a <i>valid-time</i> and a <i>preferred-time</i> value.<br>See the Usage notes below this parameter table for a description of preferred and valid lifetimes and how these determine deprecated or invalid IPv6 addresses upon expiry. |
| <code>&lt;valid-time&gt;</code>      | Specify a valid lifetime in seconds in the range <code>&lt;5-315360000&gt;</code> .   |
| <code>infinite</code>                | Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.   |
| <code>&lt;preferred-time&gt;</code>  | Specify a valid lifetime in seconds in the range <code>&lt;5-315360000&gt;</code> .   |

**Default** No IPv6 local prefix pool is specified by default.

**Mode** DHCPv6 Configuration

**Usage notes** The DHCPv6 server assigns prefixes dynamically from an IPv6 local prefix pool, which is configured using the `ipv6 local pool` command and is associated with a DHCPv6 configuration pool using this command. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes from the pool. After the client releases the previously assigned prefixes, the server returns the prefixes to the pool for reassignment.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source

address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

**Example** This example adds DHCPv6 Prefix Delegation pool pd\_pool1 to DHCPv6 pool pool1:

```
awplus# configure terminal
awplus(config)# ipv6 local pool pd_pool1 2001:0db8::/48 56
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# prefix-delegation pool pd_pool1
```

**Related commands**

- [ipv6 dhcp pool](#)
- [ipv6 local pool](#)
- [show ipv6 dhcp pool](#)



# service dhcp-relay

**Overview** This command enables the DHCP Relay Agent on the device. However, on a given IP interface, no DHCP forwarding takes place until at least one DHCP server is specified to forward/relay all clients' DHCP packets to.

The **no** variant of this command disables the DHCP Relay Agent on the device for all interfaces.

**Syntax** `service dhcp-relay`  
`no service dhcp-relay`

**Mode** Global Configuration

**Usage notes** A maximum number of 400 DHCP Relay Agents (one per interface) can be configured on the device. Once this limit has been reached, any further attempts to configure DHCP Relay Agents will not be successful.

**Default** The DHCP-relay service is enabled by default.

**Examples** To enable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
```

To disable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# no service dhcp-relay
```

**Related commands**

- [ip dhcp-relay agent-option](#)
- [ip dhcp-relay agent-option checking](#)
- [ip dhcp-relay information policy](#)
- [ip dhcp-relay maxhops](#)
- [ip dhcp-relay server-address](#)

# show counter dhcp-relay

**Overview** This command shows counters for the DHCP Relay Agent on your device.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show counter dhcp-relay

**Mode** User Exec and Privileged Exec

**Examples** To display counters for the DHCP Relay Agent on your device, use the following command:

```
awplus# show counter dhcp-relay
```

**Output** Figure 21-2: Example output from the **show counter dhcp-relay** command

```
awplus#show counter dhcp-relay

DHCP relay counters
Requests In           ..... 4
Replies In           ..... 4
Relayed To Server    ..... 4
Relayed To Client    ..... 4
Out To Server Failed ..... 0
Out To Client Failed ..... 0
Invalid hlen         ..... 0
Bogus giaddr         ..... 0
Corrupt Agent Option ..... 0
Missing Agent Option ..... 0
Bad Circuit ID       ..... 0
Missing Circuit ID    ..... 0
Bad Remote ID        ..... 0
Missing Remote ID    ..... 0
Option Insert Failed ..... 0
DHCPv6 Requests In  ..... 0
DHCPv6 Replies In   ..... 0
DHCPv6 Relayed to Server ..... 0
DHCPv6 Relayed to Client ..... 0
```

| Parameter         | Description  |
|-------------------|--|
| Requests In       | The number of DHCP Request messages received from clients. |
| Replies In        | The number of DHCP Reply messages received from servers.   |
| Relayed To Server | The number of DHCP Request messages relayed to servers.    |
| Relayed To Client | The number of DHCP Reply messages relayed to clients.      |

| Parameter            | Description  |
|----------------------|--|
| Out To Server Failed | The number of failures when attempting to send request messages to servers. This is an internal debugging counter.   |
| Out To Client Failed | The number of failures when attempting to send reply messages to clients. This is an internal debugging counter.   |
| Invalid hlen         | The number of incoming messages dropped due to an invalid hlen field.  |
| Bogus giaddr         | The number of incoming DHCP Reply messages dropped due to the bogus giaddr field.  |
| Corrupt Agent Option | The number of incoming DHCP Reply messages dropped due to a corrupt relay agent information option field. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command. |
| Missing Agent Option | The number of incoming DHCP Reply messages dropped due to a missing relay agent information option field. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command. |
| Bad Circuit ID       | The number of incoming DHCP Reply messages dropped due to a bad circuit ID. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.                               |
| Missing Circuit ID   | The number of incoming DHCP Reply messages dropped due to a missing circuit ID. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.                           |

| Parameter                | Description  |
|--------------------------|--|
| Bad Remote ID            | The number of incoming DHCP Reply messages dropped due to a bad remote ID.<br>Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command  |
| Missing Remote ID        | The number of incoming DHCP Reply messages dropped due to a missing remote ID.<br>Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command  |
| Option Insert Failed     | The number of incoming DHCP Request messages dropped due to an error adding the DHCP Relay Agent information (option-82). This counter increments when: <ul style="list-style-type: none"> <li>the DHCP Relay Agent is set to drop packets with the DHCP Relay Agent Option 82 field already filled by another DHCP Relay Agent. This policy is set with the <code>ip dhcp-relay information policy</code> command.</li> <li>there is a packet error that stops the DHCP Relay Agent from being able to append the packet with its DHCP Relay Agent Information Option (Option 82) field.</li> </ul> |
| DHCPv6 Requests In       | The number of incoming DHCPv6 Request messages.  |
| DHCPv6 Replies In        | The number of incoming DHCPv6 Reply messages.  |
| DHCPv6 Relayed to Server | The number of DHCPv6 messages relayed to the server.   |
| DHCPv6 Relayed to Client | The number of DHCPv6 messages relayed to the client.   |

# show counter ipv6 dhcp-client

**Overview** Use this command in User Exec or Privilege Exec mode to show DHCPv6 client counter information. See [show counter ipv6 dhcp-server](#) for DHCPv6 server information.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show counter ipv6 dhcp-client`

**Mode** User Exec and Privileged Exec

**Example** To display the DHCPv6 client counter information, use the command:

```
awplus# show counter ipv6 dhcp-client
```

**Output** Figure 21-3: Example output from the **show counter ipv6 dhcp-client** command

```
awplus#show counter ipv6 dhcp-client
SOLICIT out          ..... 20
ADVERTISE in         ..... 12
REQUEST out          ..... 1
CONFIRM out          ..... 0
RENEW out            ..... 0
REBIND out           ..... 0
REPLY in             ..... 0
RELEASE out          ..... 0
DECLINE out          ..... 0
INFORMATION-REQUEST out ..... 0
```

**Table 1:** Parameters in the output of the **show counter ipv6 dhcp-client** command

| Parameter    | Description   |
|--------------|---|
| SOLICIT out  | Displays the count of SOLICIT messages sent by the DHCPv6 client.       |
| ADVERTISE in | Displays the count of ADVERTISE messages received by the DHCPv6 client. |
| REQUEST out  | Displays the count of REQUEST messages sent by the DHCPv6 client.       |
| CONFIRM out  | Displays the count of CONFIRM messages sent by the DHCPv6 client.       |
| RENEW out    | Displays the count of RENEW messages sent by the DHCPv6 client.         |

**Table 1:** Parameters in the output of the **show counter ipv6 dhcp-client** command (cont.)

| Parameter               | Description   |
|-------------------------|---|
| REBIND out              | Displays the count of REBIND messages sent by the DHCPv6 client.              |
| REPLY in                | Displays the count of REPLY messages received by the DHCPv6 client.           |
| RELEASE out             | Displays the count of RELEASE messages sent by the DHCPv6 client.             |
| DECLINE out             | Displays the count of DECLINE messages sent by the DHCPv6 client.             |
| INFORMATION-REQUEST out | Displays the count of INFORMATION-REQUEST messages sent by the DHCPv6 client. |

**Related commands** [show counter ipv6 dhcp-server](#)

# show counter ipv6 dhcp-server

**Overview** Use this command in User Exec or Privileged Exec mode to show DHCPv6 server counter information. See [show counter ipv6 dhcp-client](#) for DHCPv6 client information.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show counter ipv6 dhcp-server`

**Mode** User Exec and Privileged Exec

**Example** To display the DHCPv6 server counter information, use the command:

```
awplus# show counter ipv6 dhcp-server
```

**Output** Figure 21-4: Example output from the **show counter ipv6 dhcp-server** command

```
awplus#show counter ipv6 dhcp-server
SOLICIT in          ..... 20
ADVERTISE out       ..... 12
REQUEST in          ..... 1
CONFIRM in          ..... 0
RENEW in            ..... 0
REBIND in           ..... 0
REPLY out           ..... 0
RELEASE in          ..... 0
DECLINE in          ..... 0
INFORMATION-REQUEST in ..... 0
```

**Table 2:** Parameters in the output of the **show counter ipv6 dhcp-server** command

| Parameter     | Description   |
|---------------|---|
| SOLICIT in    | Displays the count of SOLICIT messages received by the DHCPv6 server. |
| ADVERTISE out | Displays the count of ADVERTISE messages sent by the DHCPv6 server.   |
| REQUEST in    | Displays the count of REQUEST messages received by the DHCPv6 server. |
| CONFIRM in    | Displays the count of CONFIRM messages received by the DHCPv6 server. |
| RENEW in      | Displays the count of RENEW messages received by the DHCPv6 server.   |

**Table 2:** Parameters in the output of the **show counter ipv6 dhcp-server** command (cont.)

| Parameter              | Description   |
|------------------------|---|
| REBIND in              | Displays the count of REBIND messages received by the DHCPv6 server.              |
| REPLY out              | Displays the count of REPLY messages sent by the DHCPv6 server.                   |
| RELEASE in             | Displays the count of RELEASE messages received by the DHCPv6 server.             |
| DECLINE in             | Displays the count of DECLINE messages received by the DHCPv6 server.             |
| INFORMATION-REQUEST in | Displays the count of INFORMATION-REQUEST messages received by the DHCPv6 server. |

**Related commands** [show counter ipv6 dhcp-client](#)



# show ip dhcp-relay

**Overview** This command shows the configuration of the DHCP Relay Agent on each interface.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip dhcp-relay [interface <interface-name>]`

| Parameter        | Description  |
|------------------|--|
| <interface-name> | Name of a specific interface. This displays the DHCP configuration for the specified interface only. |

**Mode** User Exec and Privileged Exec

**Example** To display the DHCP Relay Agent’s configuration on the interface vlan1, use the command:

```
awplus# show ip dhcp-relay interface vlan1
```

**Output** Figure 21-5: Example output from the **show ip dhcp-relay** command

```
DHCP Relay Service is enabled

vlan1 is up, line protocol is up
Maximum hop count is 10
Insertion of Relay Agent Option is disabled
Checking of Relay Agent Option is disabled
The Remote Id string for Relay Agent Option is 0000.cd28.074c
Relay information policy is to append new relay agent
information
List of servers : 192.168.1.200
```

- Related commands**
- [ip dhcp-relay agent-option](#)
  - [ip dhcp-relay agent-option checking](#)
  - [ip dhcp-relay information policy](#)
  - [ip dhcp-relay maxhops](#)
  - [ip dhcp-relay server-address](#)

# show ipv6 dhcp

**Overview** Use this command in User Exec or Privileged Exec mode to show the DHCPv6 unique identifier (DUID) configured on your device.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 dhcp`

**Mode** User Exec and Privileged Exec

**Usage notes** The DUID is based on the link-layer address for both DHCPv6 client and DHCPv6 server identifiers. The device uses the MAC address from the lowest interface number for the DUID.

The DUID is used by a DHCPv6 client to obtain an IPv6 address from a DHCPv6 server. A DHCPv6 server compares the DUID with its database of DUIDs and sends configuration data for an IPv6 address plus the preferred and valid lease time values to a DHCPv6 client.

**Example** To display the DUID configured on your device, use the command:

```
awplus# show ipv6 dhcp
```

**Output** Figure 21-6: Example output from the **show ipv6 dhcp** command

```
awplus#show ipv6 dhcp
DHCPv6 Server DUID: 0001000117ab6876001577f7ba23
```

**Related commands** [ipv6 address dhcp](#)

# show ipv6 dhcp binding

**Overview** Use this command in User Exec or Privileged Exec mode to show the IPv6 address entries that the DHCPv6 server leases to DHCPv6 clients. Note that applying this command with the optional *summary* keyword parameter displays the number of addresses per pool, but not the address or prefix entries per pool.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 dhcp binding [summary]`

| Parameter | Description  |
|-----------|--|
| summary   | Optional. Specify the <b>summary</b> keyword to display summarized information for DHCPv6 server leases to client nodes, displaying the number of address entries per pool, not the addresses or prefixes. |

**Mode** User Exec and Privileged Exec

**Example 1** To display the total DHCPv6 leasing address entries for all pools, use the command:

```
awplus# show ipv6 dhcp binding summary
```

**Output** Figure 21-7: Example output from the **show ipv6 dhcp binding summary** command

```
awplus# show ipv6 dhcp binding summary
Pool Name                Number of Leased Addresses
-----
ia-na1                    3
ia-pd1                    5

Total in all Pools:      8
```

**Table 3:** Parameters in the output of the **show ipv6 dhcp binding summary** command

| Parameter                  | Description  |
|----------------------------|--|
| Pool Name                  | Displays a list of all the pool names.                             |
| Number of Leased Addresses | Displays the number of leased address entries for the pool.        |
| Total in all Pools         | Displays the total number of leased address entries for all pools. |

**Example 2** To display addresses, prefixes, and lifetimes for all DHCPv6 leasing entries by pool, enter:

```
awplus# show ipv6 dhcp binding
```

**Output** Figure 21-8: Example output from the **show ipv6 dhcp binding** command

```
awplus#show ipv6 dhcp binding
Pool ia-na1
  Address 2002:0:3c0::1
    client IAID 77f7ba23, DUID 0001000117c4bbb4001577f7ba23
    preferred lifetime 604800, valid lifetime 2592000
    starts at 20 Aug 2012 18:38:29
    expires at 19 Sep 2012 18:38:29
Pool ia-pd1
  Prefix 2002:0:3c0::/42
    client IAID 77f7ba23, DUID 0001000117c4bbb4001577f7ba23
    preferred lifetime 604800, valid lifetime 2592000
    starts at 20 Aug 2012 18:38:29
    expires at 19 Sep 2012 18:38:29
```

**Table 4:** Parameters in the output of the **show ipv6 dhcp binding** command

| Parameter          | Description  |
|--------------------|--|
| Address            | Address delegated to the indicated IAID and DUID. See the IAID and DUID descriptions below for further information.  |
| Prefix             | Prefix delegated to the indicated IAID and DUID. See the IAID and DUID descriptions below for further information.   |
| DUID               | DHCPv6 unique identifier (DUID) (see RFC 3315). Each DHCPv6 client has as DUID. DHCPv6 servers use DUIDs to identify clients for the association of IAs (Identity Associations) with DHCPv6 clients. DHCPv6 clients use DUIDs to identify a DHCPv6 server.   |
| IAID               | Identify Association Identifier (IAID) (see RFC 3315). IAIDs are identifiers for IAs (Identity Associations), where an IA is a collection of IPv6 addresses assigned to a DHCPv6 client. Each IA has an associated IAD. Each DHCPv6 client may have more than one IA assigned to it. Each IA holds one type of address.  |
| preferred lifetime | The preferred lifetime setting in seconds for the specified IAID and DUID. Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires. Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected. |
| valid lifetime     | The valid lifetime setting in seconds for the specified IAID and DUID. An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.  |

**Table 4:** Parameters in the output of the **show ipv6 dhcp binding** command

| Parameter  | Description  |
|------------|--|
| starts at  | The date and time at which the valid lifetime expires. |
| expires at | The date and time at which the valid lifetime expires. |

**Related  
commands**

[clear ipv6 dhcp binding](#)  
[ipv6 dhcp pool](#)  
[show ipv6 dhcp pool](#)

# show ipv6 dhcp interface

**Overview** Use this command in User Exec or Privileged Exec mode to display DHCPv6 information for a specified interface, or all interfaces when entered without the interface parameter.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 dhcp interface [<interface-name>]`

| Parameter        | Description  |
|------------------|--|
| <interface-name> | Optional. Specify the name of the interface to show DHCPv6 information about. Omit this optional parameter to display DHCPv6 information for all interfaces DHCPv6 is configured on. |

**Mode** User Exec and Privileged Exec

**Example** To display DHCPv6 information for all interfaces DHCPv6 is configured on, use the command:

```
awplus# show ipv6 dhcp interface
```

**Output** Figure 21-9: Example output from the **show ipv6 dhcp interface** command

```
awplus# show ipv6 dhcp interface
vlan1 is in client mode
Address 1001::3c0:1
    preferred lifetime 9000, valid lifetime 5000
    starts at 20 Jan 2012 09:21:35
    expires at 20 Jan 2012 10:25:32
```

**Example 2** To display DHCPv6 information for interface vlan1, use the command:

```
awplus# show ipv6 dhcp interface vlan1
```

**Output** Figure 21-10: Example output from the **show ipv6 dhcp interface** command for a specific interface

```
awplus# show ipv6 dhcp interface vlan1
vlan1 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 5:** Parameters in the output of the **show counter dhcp-client** command

| Parameter  | Description  |
|--|--|
| <interface> is in server/client/(Prefix-Delegation) mode | Displays whether the specified interface is in server or client mode and whether prefix-delegation is applied to an interface. |
| Address  | Displays the address of the DHCPv6 server on the interface.  |
| Prefix name  | Displays the IPv6 general prefix pool name, where prefixes are stored for the interface.                                       |
| Using pool   | Displays the name of the pool used by the interface.   |
| Preference   | Displays the preference value for the DHCPv6 server.   |

**Related commands** [ipv6 dhcp client pd](#)

# show ipv6 dhcp pool

**Overview** Use this command in User Exec or Privileged Exec mode to display the configuration details and system usage of the DHCPv6 address pools configured on the device.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 dhcp pool [<DHCPv6-address-pool-name>]`

| Parameter                  | Description  |
|----------------------------|--|
| <DHCPv6-address-pool-name> | Name of a specific DHCPv6 address pool. This displays the configuration of the specified DHCPv6 address pool only. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ipv6 dhcp pool`

**Output** Figure 21-11: Example output from the **show ipv6 dhcp pool** command

```
awplus# show ipv6 dhcp pool
DHCPv6 Pool: ia-na
Address Prefix : 1001::/64
    Lifetime: 2592000(valid), 604800(preferred)
DNS Server: 2001::1
DNS Server: 2001::2
Domain Name: example.com
Domain Name: example.co.jp
SNTP Server: 2001::5
SNTP Server: 2001::6
Option Code : 150
    Value: [ASCII] test-test
DHCPv6 Pool: ia-pd
PD Pool Name: pd1
Prefix : 2002::/38-42
Lifetime : 2592000(valid), 604800(preferred)
```

**Table 6:** Parameters in the output of the **show ipv6dhcp pool** command

| Parameter      | Description                        |
|----------------|------------------------------------|
| DHCPv6 Pool    | Name of the DHCPv6 pool.           |
| Address Prefix | Address prefix to the DHCPv6 pool. |



**Table 6:** Parameters in the output of the **show ipv6dhcp pool** command (cont.)

| Parameter           | Description   |
|---------------------|---|
| Address<br>Lifetime | Valid and preferred lifetimes to the DHCPv6 pool.<br>Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.<br>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.<br>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. |
| DNS Server          | IPv6 address of the DNS Server  |
| Domain name         | URL for the domain name.  |
| SNTP Server         | IPv6 address of the SNTP (Simple Network Time Protocol) Server.   |
| Option Code         | DHCP Option code (see RFC 2132).  |
| Option Value        | DHCP Option value type (see RFC 2132).  |

**Related commands** [ipv6 dhcp pool](#)

# sntp-address

**Overview** Use this command in DHCPv6 Configuration mode to add an SNTP Server IPv6 address to a DHCPv6 Server pool.

Use the **no** variant of this command to remove an SNTP Server IPv6 address from a DHCPv6 Server pool.

**Syntax** `sntp-address <ipv6-address>`  
`no sntp-address <ipv6-address>`

| Parameter                         | Description  |
|-----------------------------------|--|
| <code>&lt;ipv6-address&gt;</code> | Specify an SNTP Server IPv6 address, in hexadecimal notation in the format <code>x:x::x:x</code> . |

**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](#)

# 22

# NTP Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure the Network Time Protocol (NTP). For more information, see the [NTP Feature Overview and Configuration Guide](#).

The device can act as an NTP client to receive time from one or more NTP servers, and as an NTP server.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare\\_Plus” Feature Overview and Configuration Guide](#).

- Command List**
- [“ntp authenticate”](#) on page 1036
  - [“ntp authentication-key”](#) on page 1037
  - [“ntp broadcastdelay”](#) on page 1038
  - [“ntp discard”](#) on page 1039
  - [“ntp master”](#) on page 1040
  - [“ntp peer”](#) on page 1041
  - [“ntp rate-limit”](#) on page 1043
  - [“ntp restrict”](#) on page 1044
  - [“ntp server”](#) on page 1046
  - [“ntp source”](#) on page 1048
  - [“ntp trusted-key \(deprecated\)”](#) on page 1050
  - [“show counter ntp \(deprecated\)”](#) on page 1051
  - [“show ntp associations”](#) on page 1052
  - [“show ntp counters”](#) on page 1054
  - [“show ntp counters associations”](#) on page 1055
  - [“show ntp status”](#) on page 1056

# ntp authenticate

**Overview** This command enables NTP authentication. This allows NTP to authenticate the associations with other systems for security purposes.

The **no** variant of this command disables NTP authentication.

**Syntax** ntp authenticate  
no ntp authenticate

**Mode** Global Configuration

**Examples** To enable NTP authentication, use the commands:

```
awplus# configure terminal  
awplus(config)# ntp authenticate
```

To disable NTP authentication, use the commands:

```
awplus# configure terminal  
awplus(config)# no ntp authenticate
```

# ntp authentication-key

**Overview** This command defines each of the authentication keys. Each key has a key number, a type (MD5 or SHA1), and a value.

The **no** variant of this disables the authentication key.

**Syntax** `ntp authentication-key <keynumber> {md5|sha1} <key> [trusted]`  
`no ntp authentication-key <keynumber>`

| Parameter   | Description  |
|-------------|--|
| <keynumber> | <1-4294967295> An identification number for the key.   |
| md5         | Define an MD5 key.   |
| sha1        | Define an SHA1 key.  |
| <key>       | The authentication key. For SHA1, this is a 20 hexadecimal character string. For MD5, this is a string of up to 31 ASCII characters. |
| trusted     | Add this key to the list of authentication keys that this server trusts.   |

**Mode** Global Configuration

**Examples** To define an MD5 authentication key number 134343 and a key value "mystring", use the commands:

```
awplus# configure terminal  
awplus(config)# ntp authentication-key 134343 md5 mystring
```

To disable the authentication key number 134343 with the key value "mystring", use the commands:

```
awplus# configure terminal  
awplus(config)# no ntp authentication-key 134343 md5 mystring
```

# ntp broadcastdelay

**Overview** Use this command to set the estimated round-trip delay for broadcast packets. Use the **no** variant of this command to reset the round-trip delay for broadcast packets to the default offset of 0 microseconds.

**Syntax** `ntp broadcastdelay <delay>`  
`no ntp broadcastdelay`

| Parameter | Description                                     |
|-----------|---|
| <delay>   | <1-999999> The broadcast delay in microseconds. |

**Default** 0 microsecond offset, which can only be applied with the **no** variant of this command.

**Mode** Global Configuration

**Examples** To set the estimated round-trip delay to 23464 microseconds for broadcast packets, use these commands:

```
awplus# configure terminal
awplus(config)# ntp broadcastdelay 23464
```

To reset the estimated round-trip delay for broadcast packets to the default setting (0 microseconds), use these commands:

```
awplus# configure terminal
awplus(config)# no ntp broadcastdelay
```

# ntp discard

**Overview** Use this command to limit the time between NTP packets on the host or hosts specified by the command [ntp restrict](#). Packets that arrive at greater frequency than the limits are dropped or sent a kiss-of-death response.

Use the **no** variant of this command to return the limits to their default values.

**Syntax**

```
ntp discard minimum <1-60>
ntp discard average <1-16>
no ntp discard minimum
no ntp discard average
```

| Parameter      | Description   |
|----------------|---|
| minimum <1-60> | The minimum time between NTP packets, in seconds.   |
| average <1-16> | A value that determines the minimum average time between NTP packets. The number of seconds is 2 to the power of the specified value (e.g. if you specify 4, the minimum average time is 16 seconds). |

**Default** Minimum: 2  
Average: 3 (8 seconds)

**Mode** Global Configuration

**Example** To drop NTP packets from the 192.168.1.0/16 subnet if they arrive more frequently than every 5 seconds, and also send kiss-of-death messages, use the commands:

```
awplus# configure terminal
awplus(config)# ntp discard minimum 5
awplus(config)# ntp restrict 192.168.1.0/16 limited kod
```

To silently drop all NTP packets if they arrive more frequently than once every 4 seconds on average (2 to the power of 2), use the commands:

```
awplus# configure terminal
awplus(config)# ntp discard average 2
awplus(config)# ntp restrict default-v4 limited
awplus(config)# ntp restrict default-v6 limited
```

**Related commands** [ntp restrict](#)

# ntp master

**Overview** Use this command to make the device to be an authoritative NTP server, even if the system is not synchronized to an outside time source.

Use the **no** variant of this command to stop the device being the designated NTP server.

**Syntax** `ntp master [<stratum>]`  
`no ntp master`

| Parameter                    | Description   |
|------------------------------|---|
| <code>&lt;stratum&gt;</code> | <code>&lt;1-15&gt;</code> The stratum number defines the configured level that is set for this master within the NTP hierarchy. The default stratum number is 12. |

**Mode** Global Configuration

**Usage notes** The stratum levels define the distance from the reference clock and exist to prevent cycles in the hierarchy. Stratum 1 is used to indicate time servers, which are more accurate than Stratum 2 servers. For more information on the Network Time Protocol go to: [www.ntp.org](http://www.ntp.org)

**Examples** To stop the device from being the designated NTP server, use the commands:

```
awplus# configure terminal  
awplus(config)# no ntp master
```

To make the device the designated NTP server with stratum number 2, use the commands:

```
awplus# configure terminal  
awplus(config)# ntp master 2
```



# ntp peer

**Overview** Use this command to configure an NTP peer association. An NTP association is a peer association if this system is willing to either synchronize to the other system, or allow the other system to synchronize to it.

Use the **no** variant of this command to remove the configured NTP peer association.

**Syntax**

```
ntp peer {<peeraddress>|<peername>}
ntp peer {<peeraddress>|<peername>} [prefer] [key <key>]
[version <version>]
no ntp peer {<peeraddress>|<peername>}
```

| Parameter         | Description   |
|-------------------|---|
| <peeraddress>     | Specify the IP address of the peer, entered in the form A.B.C.D for an IPv4 address, or in the form X:X::X:X for an IPv6 address. |
| <peername>        | Specify the peer hostname. The peer hostname can resolve to an IPv4 and an IPv6 address.  |
| prefer            | Prefer this peer when possible.   |
| key <key>         | <1-4294967295><br>Configure the peer authentication key.  |
| version <version> | <1-4><br>Configure for this NTP version.  |

**Mode** Global Configuration

**Examples** See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv4 address of 192.0.2.23:

```
awplus# configure terminal
awplus(config)# ntp peer 192.0.2.23
awplus(config)# ntp peer 192.0.2.23 prefer
awplus(config)# ntp peer 192.0.2.23 prefer version 4
awplus(config)# ntp peer 192.0.2.23 prefer version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4
awplus(config)# ntp peer 192.0.2.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of 192.0.2.23, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 192.0.2.23
```

See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv6 address of 2001:0db8:010d::1:

```
awplus# configure terminal
awplus(config)# ntp peer 2001:0db8:010d::1
awplus(config)# ntp peer 2001:0db8:010d::1 prefer
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4 key
1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4 key 1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4
awplus(config)# ntp peer 2001:0db8:010d::1 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of 2001:0db8:010d::1, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 2001:0db8:010d::1
```

**Related  
commands**    [ntp server](#)  
              [ntp source](#)

# ntp rate-limit

**Overview** Use this command to enable NTP server response rate-limiting. Limiting NTP server responses can reduce network traffic when occurrences such as misconfigured or broken NTP clients poll the NTP server too frequently. Excessive polling can lead to network overload.

Use the **no** variant of this command to remove the rate-limit configuration.

**Syntax** `ntp rate-limit {interval<1-4096>|burst <1-255>|leak <2-16>}`  
`no ntp rate-limit`

| Parameter | Description  |
|-----------|--|
| interval  | The minimum interval between responses configured in seconds. The default interval is 8 seconds.   |
| burst     | The maximum number of responses that can be sent in a burst, temporarily exceeding the limit specified by the interval option. The default burst is 8 responses.   |
| leak      | The rate at which responses are randomly allowed even if the limits specified by the interval and burst options are exceeded. The default leak is 4, i.e. on average, every fourth request has a response. |

**Mode** Global Configuration

**Default** Interval - 8 seconds.

Burst - 8 responses.

Leak - 4.

**Example** To configure an NTP rate-limiting interval of 30 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# ntp rate-limit interval 30
```

**Related commands** [ntp restrict](#)

**Command changes** Version 5.4.8-1.1: command added

# ntp restrict

**Overview** Use this command to configure a restriction (allow or deny) on NTP packets or NTP functionality for a specific host/network or all hosts of a given IP family.

This means you can control host access to NTP service and NTP server status queries.

Use the **no** variant of this command to remove a restriction from one or more hosts.

**Syntax**

```
ntp restrict
{default-v4|default-v6|<host-address>|<host-subnet>}
{allow|deny}

ntp restrict
{default-v4|default-v6|<host-address>|<host-subnet>} query
{allow|deny}

ntp restrict
{default-v4|default-v6|<host-address>|<host-subnet>} serve
{allow|deny}

no ntp restrict
{default-v4|default-v6|<host-address>|<host-subnet>}
```

| Parameter      | Description  |
|----------------|--|
| default-v4     | Apply this restriction to all IPv4 hosts.  |
| default-v6     | Apply this restriction to all IPv6 hosts.  |
| <host-address> | Apply this restriction to the specified IPv4 or IPv6 host.<br>Enter an IPv4 address in the format A.B.C.D.<br>Enter an IPv6 address in the format X::X:X.            |
| <host-subnet>  | Apply this restriction to the specified IPv4 subnet or IPv6 prefix.<br>Enter an IPv4 subnet in the format A.B.C.D/M.<br>Enter an IPv6 prefix in the format X::X:X/X. |
| query          | Control NTP server status queries to matching hosts.   |
| serve          | Control NTP time service to matching hosts.  |
| allow          | Allow the configured restriction.  |
| deny           | Deny the configured restriction.   |

**Default** By default, time service is allowed to all hosts, and NTP server status querying is denied to all hosts.

**Mode** Global Configuration

**Example** To prevent all IPv4 hosts from accessing a device for NTP service, use the commands:

```
awplus# configure terminal
awplus(config)# ntp restrict default-v4 deny
```

To prevent the host 192.168.1.1 from accessing a device for NTP service, use the commands:

```
awplus# configure terminal
awplus(config)# ntp restrict 198.168.1.1 deny
```

To allow all hosts in the 10.10.10.0/24 subnet to access a device for NTP server status, use the commands:

```
awplus# configure terminal
awplus(config)# ntp restrict 10.10.10.0/24 query allow
```

**Related commands** [ntp rate-limit](#)

**Command changes** Version 5.4.8-1.1: command added

# ntp server

**Overview** Use this command to configure an NTP server. This means that this system will synchronize to the other system, and not vice versa.

Use the **no** variant of this command to remove the configured NTP server.

**Syntax** `ntp server {<serveraddress>|<servername>}`  
`ntp server {<serveraddress>|<servername>} [prefer] [key <key>] [version <version>]`  
`no ntp server {<serveraddress>|<servername>}`

| Parameter         | Description  |
|-------------------|--|
| <serveraddress>   | Specify the IP address of the peer, entered in the form A . B . C . D for an IPv4 address, or in the form X : X : : X . X for an IPv6 address. |
| <servername>      | Specify the server hostname. The server hostname can resolve to an IPv4 and an IPv6 address.   |
| prefer            | Prefer this server when possible.  |
| key <key>         | <1-4294967295><br>Configure the server authentication key.   |
| version <version> | <1-4><br>Configure for this NTP version.   |

**Mode** Global Configuration

**Examples** See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv4 address of 192.0.1.23:

```
awplus# configure terminal
awplus(config)# ntp server 192.0.1.23
awplus(config)# ntp server 192.0.1.23 prefer
awplus(config)# ntp server 192.0.1.23 prefer version 4
awplus(config)# ntp server 192.0.1.23 prefer version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4
awplus(config)# ntp server 192.0.1.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of 192.0.1.23, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp server 192.0.1.23
```

See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv6 address of 2001:0db8:010e::2:

```
awplus# configure terminal
awplus(config)# ntp server 2001:0db8:010e::2
awplus(config)# ntp server 2001:0db8:010e::2 prefer
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4 key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4
awplus(config)# ntp server 2001:0db8:010e::2 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of 2001:0db8:010e::2, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp server 2001:0db8:010e::2
```

**Related  
commands**    [ntp peer](#)  
                  [ntp source](#)

# ntp source

**Overview** Use this command to configure an IPv4 or an IPv6 address for the NTP source interface. This command defines the socket used for NTP messages, and only applies to NTP client behavior.

Note that you cannot use this command when using AMF (Allied Telesis Management Framework).

Use the **no** variant of this command to remove the configured IPv4 or IPv6 address from the NTP source interface.

**Syntax** `ntp source <source-address>`  
`no ntp source`

| Parameter                           | Description   |
|-------------------------------------|---|
| <code>&lt;source-address&gt;</code> | Specify the IP address of the NTP source interface, entered in the form A.B.C.D for an IPv4 address, or in the form X:X::X.X for an IPv6 address. |

**Default** An IP address is selected based on the most appropriate egress interface used to reach the NTP peer if a configured NTP client source IP address is unavailable or invalid.

**Mode** Global Configuration

**Usage notes** Adding an IPv4 or an IPv6 address allows you to select which source interface NTP uses for peering. The IPv4 or IPv6 address configured using this command is matched to the interface.

When selecting a source IP address to use for NTP messages to the peer, if the configured NTP client source IP address is unavailable then default behavior will apply, and an alternative source IP address is automatically selected. This IP address is based on the most appropriate egress interface used to reach the NTP peer. The configured NTP client source IP may be unavailable if the interface is down, or an invalid IP address is configured that does not reside on the device.

Note that this command only applies to NTP client behavior. The egress interface that the NTP messages use to reach the NTP server is determined by the `ntp peer` and `ntp server` commands.

Note that you cannot use this command when using AMF (Allied Telesis Management Framework).

**Examples** To configure the NTP source interface with the IPv4 address 192.0.2.23, enter the commands:

```
awplus# configure terminal
awplus(config)# ntp source 192.0.2.23
```



To configure the NTP source interface with the IPv6 address 2001:0db8:010e::2, enter the commands:

```
awplus# configure terminal  
awplus(config)# ntp source 2001:0db8:010e::2
```

To remove a configured address for the NTP source interface, use the following commands:

```
awplus# configure terminal  
awplus(config)# no ntp source
```

**Related commands**

- [ntp peer](#)
- [ntp server](#)

## ntp trusted-key (deprecated)

**Overview** This command has been deprecated in Software Version 5.4.6-1.1. Please use the **trusted** parameter of the command [ntp authentication-key](#) instead.

# show counter ntp (deprecated)

**Overview** From version 5.4.6-1.x onwards, this command has been replaced by the command [show ntp counters](#).

# show ntp associations

**Overview** Use this command to display the status of NTP associations.

**Syntax** show ntp associations

**Mode** User Exec and Privileged Exec

**Example** See the sample output of the **show ntp associations** command displaying the status of NTP associations.

Table 22-1: Example output from **show ntp associations**

```
awplus#show ntp associations
remote          refid          st t when poll reach  delay  offset  disp
-----
*server1.example.com
                192.0.2.2      4 u  47  64  377  0.177  0.021  0.001
+192.168.1.10   10.32.16.80   5 u  46  64  377  0.241  -0.045 0.000
* system peer, # backup, + candidate, - outlier, x false ticker
```

Table 22-2: Parameters in the output from **show ntp associations**

| Parameter      | Description  |
|----------------|--|
| * system peer  | The peer that NTP uses to calculate variables like the offset and root dispersion of this AlliedWare Plus device. NTP passes these variables to the clients using this AlliedWare Plus device.   |
| # backup       | Peers that are usable, but are not among the first six peers sorted by synchronization distance. These peers may not be used.  |
| + candidate    | Peers that the NTP algorithm has determined can be used, along with the system peer, to discipline the clock (i.e. to set the time on the AlliedWare Plus device).   |
| - outlier      | Peers that are not used because their time is significantly different from the other peers.  |
| x false ticker | Peers that are not used because they are not consider trustworthy.   |
| space          | Peers that are not used because they are, for example, unreachable.  |
| remote         | The peer IP address  |
| refid          | The IP address of the reference clock, or an abbreviation indicating the type of clock (e.g. GPS indicates that the server uses GPS for the reference clock). INIT indicates that the reference clock is initializing, so it is not operational. |

Table 22-2: Parameters in the output from **show ntp associations** (cont.)

| Parameter | Description  |
|-----------|--|
| st        | The stratum, which is the number of hops between the server and the accurate time source such as an atomic clock.  |
| t         | Type, one of:<br>u: unicast or anycast client<br>b: broadcast or multicast client<br>l: local reference clock<br>s: symmetric peer<br>A: anycast server<br>B: broadcast server<br>M: multicast server  |
| when      | When last polled (seconds ago, h hours ago, or d days ago).  |
| poll      | Time between NTP requests from the device to the server.   |
| reach     | An indication of whether or not the NTP server is responding to requests. 0 indicates there has never been a successful poll; 1 indicates that the last poll was successful; 3 indicates that the last two polls were successful; 377 indicates that the last 8 polls were successful. |
| delay     | The round trip communication delay to the remote peer or server, in milliseconds.  |
| offset    | The mean offset (phase) in the times reported between this local host and the remote peer or server (root mean square, milliseconds).  |
| disp      | The amount of clock error (in milliseconds) of the server due to clock resolution, network congestion, etc.  |

# show ntp counters

**Overview** This command displays packet counters for NTP.

**Syntax** show ntp counters

**Mode** Privileged Exec

**Example** To display counters for NTP use the command:

```
awplus# show ntp counters
```

Figure 22-1: Example output from **show ntp counters**

```
awplus#show ntp counters
Server Received          4
Server Dropped          0
Client Sent             90
Client Received         76
Client Valid Received   76
```

Table 22-3: Parameters in the output from **show ntp counters**

| Parameter             | Description  |
|-----------------------|--|
| Server Received       | Number of NTP packets received from NTP clients.             |
| Server Dropped        | Number of NTP packets received from NTP clients but dropped. |
| Client Sent           | Number of NTP packets sent to servers.                       |
| Client Received       | Number of NTP packets received from servers                  |
| Client Valid Received | Number of valid NTP packets received from servers.           |

# show ntp counters associations

**Overview** Use this command to display NTP packet counters for individual servers and peers.

**Syntax** show ntp counters associations

**Mode** Privileged Exec

**Examples** To display packet counters for each NTP server and peer that is associated with a device, use the command:

```
awplus# show ntp counters associations
```

**Output** Figure 22-2: Example output from **show ntp counters associations**

```
awplus#show ntp counters associations
Peer 2001::1
  sent:          -
  received:      -
Peer 10.37.219.100
  sent:          7
  received:      7
```

Table 22-4: Parameters in the output from **show ntp counters associations**

| Parameter | Description  |
|-----------|--|
| Peer      | An NTP peer or server that the device is associated with.          |
| sent      | The number of NTP packets that this device sent to the peer.       |
| received  | The number of NTP packets that this device received from the peer. |

**Related commands** [ntp discard](#)  
[ntp restrict](#)

# show ntp status

**Overview** Use this command to display the status of the Network Time Protocol (NTP).

**Syntax** show ntp status

**Mode** User Exec and Privileged Exec

**Example** To see information about NTP status, use the command:

```
awplus# show ntp status
```

For information about the output displayed by this command, see [ntp.org](http://ntp.org).

Figure 22-3: Example output from **show ntp status**

```
awplus#show ntp status
Reference ID   : COA8010A (192.168.1.10)
Stratum       : 4
Ref time (UTC) : Fri Jun 15 05:32:38 2018
System time   : 0.000002004 seconds fast of NTP time
Last offset   : -0.002578615 seconds
RMS offset    : 0.000928071 seconds
Frequency     : 5.099 ppm slow
Residual freq : -9.120 ppm
Skew          : 17.486 ppm
Precision     : -21 (0.000000477 seconds)
Root delay    : 0.031749818 seconds
Root dispersion : 0.133974627 seconds
Update interval : 65.3 seconds
Leap status   : Normal
```



# 23

# SNMP Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure SNMP. For more information, see:

- the [Support for Allied Telesis Enterprise\\_MIBs in AlliedWare Plus](#), for information about which MIB objects are supported.
- the [SNMP Feature Overview and Configuration\\_Guide](#).

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

- Command List**
- [“alias \(interface\)”](#) on page 1059
  - [“debug snmp”](#) on page 1060
  - [“show counter snmp-server”](#) on page 1061
  - [“show debugging snmp”](#) on page 1065
  - [“show running-config snmp”](#) on page 1066
  - [“show snmp-server”](#) on page 1067
  - [“show snmp-server community”](#) on page 1068
  - [“show snmp-server group”](#) on page 1069
  - [“show snmp-server user”](#) on page 1070
  - [“show snmp-server view”](#) on page 1071
  - [“snmp trap link-status”](#) on page 1072
  - [“snmp trap link-status suppress”](#) on page 1073
  - [“snmp-server”](#) on page 1075
  - [“snmp-server community”](#) on page 1077
  - [“snmp-server contact”](#) on page 1078
  - [“snmp-server enable trap”](#) on page 1079

- [“snmp-server engineID local”](#) on page 1081
- [“snmp-server engineID local reset”](#) on page 1083
- [“snmp-server group”](#) on page 1084
- [“snmp-server host”](#) on page 1086
- [“snmp-server legacy-ifadminstatus”](#) on page 1088
- [“snmp-server location”](#) on page 1089
- [“snmp-server source-interface”](#) on page 1090
- [“snmp-server startup-trap-delay”](#) on page 1091
- [“snmp-server user”](#) on page 1092
- [“snmp-server view”](#) on page 1095
- [“undebg snmp”](#) on page 1096

# alias (interface)

**Overview** Use this command to set an alias name for a port, as returned by the SNMP ifMIB in OID 1.3.6.1.2.1.31.1.1.1.18.

Use the **no** variant of this command to remove an alias name from a port.

**Syntax** `alias <ifAlias>`  
`no alias`

| Parameter                    | Description  |
|------------------------------|--|
| <code>&lt;ifAlias&gt;</code> | 64 character name for an interface in a network management system. All printable characters are valid. |

**Default** Not set.

**Mode** Interface Configuration

**Usage notes** The interface alias can also be set via SNMP.

Third-party management systems often use standard MIBs to access device information. Network managers can specify an alias interface name to provide a non-volatile way to access the interface.

**Example** To configure the alias interface name "uplink\_a" for port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# alias uplink_a
```

To remove an alias interface name from port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no alias
```

**Command changes** Version 5.4.8-2.1: command added

# debug snmp

**Overview** This command enables SNMP debugging.

The **no** variant of this command disables SNMP debugging.

**Syntax**

```
debug snmp  
[all|detail|error-string|process|receive|send|xdump]  
  
no debug snmp  
[all|detail|error-string|process|receive|send|xdump]
```

| Parameter    | Description   |
|--------------|---|
| all          | Enable or disable the display of all SNMP debugging information.                          |
| detail       | Enable or disable the display of detailed SNMP debugging information.                     |
| error-string | Enable or disable the display of debugging information for SNMP error strings.            |
| process      | Enable or disable the display of debugging information for processed SNMP packets.        |
| receive      | Enable or disable the display of debugging information for received SNMP packets.         |
| send         | Enable or disable the display of debugging information for sent SNMP packets.             |
| xdump        | Enable or disable the display of hexadecimal dump debugging information for SNMP packets. |

**Mode** Privileged Exec and Global Configuration

**Example** To start SNMP debugging, use the command:

```
awplus# debug snmp
```

To start SNMP debugging, showing detailed SNMP debugging information, use the command:

```
awplus# debug snmp detail
```

To start SNMP debugging, showing all SNMP debugging information, use the command:

```
awplus# debug snmp all
```

**Related commands**

- [show debugging snmp](#)
- [terminal monitor](#)
- [undebug snmp](#)

# show counter snmp-server

**Overview** This command displays counters for SNMP messages received by the SNMP agent.

**Syntax** show counter snmp-server

**Mode** User Exec and Privileged Exec

**Example** To display the counters for the SNMP agent, use the command:

```
awplus# show counter snmp-server
```

**Output** Figure 23-1: Example output from the **show counter snmp-server** command

```
SNMP-SERVER counters
inPkts                ..... 11
inBadVersions         ..... 0
inBadCommunityNames  ..... 0
inBadCommunityUses   ..... 0
inASNParseErrs       ..... 0
inTooBigs             ..... 0
inNoSuchNames        ..... 0
inBadValues          ..... 0
inReadOnlys          ..... 0
inGenErrs            ..... 0
inTotalReqVars       ..... 9
inTotalSetVars       ..... 0
inGetRequests        ..... 2
inGetNexts           ..... 9
inSetRequests        ..... 0
inGetResponses       ..... 0
inTraps              ..... 0
outPkts              ..... 11
outTooBigs           ..... 0
outNoSuchNames       ..... 2
outBadValues         ..... 0
outGenErrs           ..... 0
outGetRequests       ..... 0
outGetNexts          ..... 0
outSetRequests       ..... 0
outGetResponses      ..... 11
outTraps             ..... 0
UnsupportedSecLevels ..... 0
NotInTimeWindows     ..... 0
UnknownUserNames     ..... 0
UnknownEngineIDs     ..... 0
WrongDigest          ..... 0
DecryptionErrors     ..... 0
UnknownSecModels     ..... 0
InvalidMsgs          ..... 0
UnknownPDUHandlers   ..... 0
```

**Table 1:** Parameters in the output of the **show counter snmp-server** command

| Parameter           | Meaning  |
|---------------------|--|
| inPkts              | The total number of SNMP messages received by the SNMP agent.  |
| inBadVersions       | The number of messages received by the SNMP agent for an unsupported SNMP version. It drops these messages. The SNMP agent on your device supports versions 1, 2C, and 3.  |
| inBadCommunityNames | The number of messages received by the SNMP agent with an unrecognized SNMP community name. It drops these messages.   |
| inBadCommunityUses  | The number of messages received by the SNMP agent where the requested SNMP operation is not permitted from SNMP managers using the SNMP community named in the message.  |
| inASNParseErrs      | The number of ASN.1 or BER errors that the SNMP agent has encountered when decoding received SNMP Messages.  |
| inTooBigs           | The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'tooBig'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.   |
| inNoSuchNames       | The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'noSuchName'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.   |
| inBadValues         | The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'badValue'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.   |
| inReadOnlys         | The number of valid SNMP PDUs received by the SNMP agent where the value of the error-status field is 'readOnly'. The SNMP manager should not generate a PDU which contains the value 'readOnly' in the error-status field. This indicates that there is an incorrect implementations of the SNMP. |
| inGenErrs           | The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'genErr'.  |

**Table 1:** Parameters in the output of the **show counter snmp-server** command

| Parameter      | Meaning  |
|----------------|--|
| inTotalReqVars | The number of MIB objects that the SNMP agent has successfully retrieved after receiving valid SNMP Get-Request and Get-Next PDUs.   |
| inTotalSetVars | The number of MIB objects that the SNMP agent has successfully altered after receiving valid SNMP Set-Request PDUs.  |
| inGetRequests  | The number of SNMP Get-Request PDUs that the SNMP agent has accepted and processed.  |
| inGetNexts     | The number of SNMP Get-Next PDUs that the SNMP agent has accepted and processed.   |
| inSetRequests  | The number of SNMP Set-Request PDUs that the SNMP agent has accepted and processed.  |
| inGetResponses | The number of SNMP Get-Response PDUs that the SNMP agent has accepted and processed.   |
| inTraps        | The number of SNMP Trap PDUs that the SNMP agent has accepted and processed.   |
| outPkts        | The number of SNMP Messages that the SNMP agent has sent.  |
| outTooBigs     | The number of SNMP PDUs that the SNMP agent has generated with the value 'tooBig' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.     |
| outNoSuchNames | The number of SNMP PDUs that the SNMP agent has generated with the value 'noSuchName' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager. |
| outBadValues   | The number of SNMP PDUs that the SNMP agent has generated with the value 'badValue' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.   |
| outGenErrs     | The number of SNMP PDUs that the SNMP agent has generated with the value 'genErr' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.     |
| outGetRequests | The number of SNMP Get-Request PDUs that the SNMP agent has generated.   |

**Table 1:** Parameters in the output of the **show counter snmp-server** command

| Parameter                 | Meaning   |
|---------------------------|---|
| outGetNexts               | The number of SNMP Get-Next PDUs that the SNMP agent has generated.   |
| outSetRequests            | The number of SNMP Set-Request PDUs that the SNMP agent has generated.  |
| outGetResponses           | The number of SNMP Get-Response PDUs that the SNMP agent has generated.   |
| outTraps                  | The number of SNMP Trap PDUs that the SNMP agent has generated.   |
| UnsupportedSecurityLevels | The number of received packets that the SNMP agent has dropped because they requested a securityLevel unknown or not available to the SNMP agent. |
| NotInTimeWindows          | The number of received packets that the SNMP agent has dropped because they appeared outside of the authoritative SNMP agent's window.            |
| UnknownUserNames          | The number of received packets that the SNMP agent has dropped because they referenced an unknown user.   |
| UnknownEngineIDs          | The number of received packets that the SNMP agent has dropped because they referenced an unknown snmpEngineID.                                   |
| WrongDigest               | The number of received packets that the SNMP agent has dropped because they didn't contain the expected digest value.                             |
| DecryptionErrors          | The number of received packets that the SNMP agent has dropped because they could not be decrypted.   |
| UnknownSecModels          | The number of messages received that contain a security model that is not supported by the server. Valid for SNMPv3 messages only.                |
| InvalidMsgs               | The number of messages received where the security model is supported but the authentication fails. Valid for SNMPv3 messages only.               |
| UnknownPDUHandlers        | The number of times the SNMP handler has failed to process a PDU. This is a system debugging counter.   |

**Related commands** [show snmp-server](#)



# show debugging snmp

**Overview** This command displays whether SNMP debugging is enabled or disabled.

**Syntax** `show debugging snmp`

**Mode** User Exec and Privileged Exec

**Example** To display the status of SNMP debugging, use the command:

```
awplus# show debugging snmp
```

**Output** Figure 23-2: Example output from the **show debugging snmp** command

```
Sntp (SMUX) debugging status:  
Sntp debugging is on
```

**Related commands** [debug snmp](#)

# show running-config snmp

**Overview** This command displays the current configuration of SNMP on your device.

**Syntax** `show running-config snmp`

**Mode** Privileged Exec

**Example** To display the current configuration of SNMP on your device, use the command:

```
awplus# show running-config snmp
```

**Output** Figure 23-3: Example output from the **show running-config snmp** command

```
snmp-server contact AlliedTelesis
snmp-server location Philippines
snmp-server group grou1 auth read view1 write view1 notify view1
snmp-server view view1 1 included
snmp-server community public
snmp-server user user1 group1 auth md5 password priv des
password
```

**Related commands** [show snmp-server](#)

# show snmp-server

**Overview** This command displays the status and current configuration of the SNMP server.

**Syntax** `show snmp-server`

**Mode** Privileged Exec

**Example** To display the status of the SNMP server, use the command:

```
awplus# show snmp-server
```

**Output** Figure 23-4: Example output from the **show snmp-server** command

```
SNMP Server ..... Enabled
IP Protocol ..... IPv4
SNMPv3 Engine ID (configured name) ... Not set
SNMPv3 Engine ID (actual) ..... 0x80001f888021338e4747b8e607
```

- Related commands**
- [debug snmp](#)
  - [show counter snmp-server](#)
  - [snmp-server](#)
  - [snmp-server engineID local](#)
  - [snmp-server engineID local reset](#)

# show snmp-server community

**Overview** This command displays the SNMP server communities configured on the device. SNMP communities are specific to v1 and v2c.

**Syntax** `show snmp-server community`

**Mode** Privileged Exec

**Example** To display the SNMP server communities, use the command:

```
awplus# show snmp-server community
```

**Output** Figure 23-5: 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 23-6: 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 23-7: Example output from the **show snmp-server user** command

| Name   | Group name   | Auth | Privacy |
|--------|--------------|------|---------|
| freddy | guireadgroup | none | none    |

**Related commands** [show snmp-server](#)  
[snmp-server user](#)

# show snmp-server view

**Overview** This command displays the SNMP server views and is used with SNMP version 3 only.

**Syntax** `show snmp-server view`

**Mode** Privileged Exec

**Example** To display the SNMP server views configured on the device, use the command:

```
awplus# show snmp-server view
```

**Output** Figure 23-8: Example output from the **show snmp-server view** command

```
SNMP view information:
View Name ..... view1
OID ..... 1
Type ..... included
```

**Related commands** [show snmp-server](#)  
[snmp-server view](#)

# snmp trap link-status

**Overview** Use this command to enable SNMP to send link status notifications (traps) for the interfaces when an interface goes up (linkUp) or down (linkDown).

Use the **no** variant of this command to disable the sending of link status notifications.

**Syntax** `snmp trap link-status [enterprise]`  
`no snmp trap link-status`

| Parameter  | Description  |
|------------|--|
| enterprise | Send an Allied Telesis enterprise type of link trap. |

**Default** By default, link status notifications are disabled.

**Mode** Interface Configuration

**Usage notes** The link status notifications can be enabled for the following interface types:

- switch port (e.g. port1.0.1)
- VLAN (e.g. vlan1)
- Ethernet (e.g. eth1)

To specify where notifications are sent, use the [snmp-server host](#) command. To configure the device globally to send other notifications, use the [snmp-server enable trap](#) command.

**Examples** To enable SNMP to send link status notifications for port1.0.1 to port1.0.3 use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.3
awplus(config-if)# snmp trap link-status
```

To disable the sending of link status notifications for port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no snmp trap link-status
```

**Related commands** [show interface](#)  
[snmp trap link-status suppress](#)  
[snmp-server enable trap](#)  
[snmp-server host](#)



# snmp trap link-status suppress

**Overview** Use this command to enable the suppression of link status notifications (traps) for the interfaces beyond the specified threshold, in the specified interval.

Use the **no** variant of this command to disable the suppression of link status notifications for the ports.

**Syntax** `snmp trap link-status suppress {time {<1-60>|default}|threshold {<1-20>|default}}`

`no snmp trap link-status suppress`

| Parameter | Description   |
|-----------|---|
| time      | Set the suppression timer for link status notifications.  |
| <1-60>    | The suppress time in seconds.   |
| default   | The default suppress time in seconds (60).  |
| threshold | Set the suppression threshold for link status notifications. This is the number of link status notifications after which to suppress further notifications within the suppression timer interval. |
| <1-20>    | The number of link status notifications.  |
| default   | The default number of link status notifications (20).   |

**Default** By default, if link status notifications are enabled (they are enabled by default), the suppression of link status notifications is enabled: notifications that exceed the notification threshold (default 20) within the notification timer interval (default 60 seconds) are not sent.

**Mode** Interface Configuration

**Usage notes** An unstable network can generate many link status notifications. When notification suppression is enabled, a suppression timer is started when the first link status notification of a particular type (linkUp or linkDown) is sent for an interface. If the threshold number of notifications of this type is sent before the timer reaches the suppress time, any further notifications of this type generated for the interface during the interval are not sent. At the end of the interval, the sending of link status notifications resumes, until the threshold is reached in the next interval.

**Examples** To suppress link status notifications for port1.0.1 to port1.0.3 after 10 notifications in 40 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.3
awplus(config-if)# snmp trap link-status suppress time 40
threshold 10
```

To stop suppressing link status notifications for port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no snmp trap link-status suppress
```

**Related commands**

- [show interface](#)
- [snmp trap link-status](#)

# snmp-server

**Overview** Use this command to enable the SNMP agent (server) on the device. The SNMP agent receives and processes SNMP packets sent to the device, and generates notifications (traps) that have been enabled by the [snmp-server enable trap](#) command.

Use the **no** variant of this command to disable the SNMP agent on the device. When SNMP is disabled, SNMP packets received by the device are discarded, and no notifications are generated. This does not remove any existing SNMP configuration.

**Syntax** `snmp-server [ip|ipv6]`  
`no snmp-server [ip|ipv6]`

| Parameter | Description                                |
|-----------|--|
| ip        | Enable or disable the SNMP agent for IPv4. |
| ipv6      | Enable or disable the SNMP agent for IPv6. |

**Default** By default, the SNMP agent is enabled for both IPv4 and IPv6. If neither the **ip** parameter nor the **ipv6** parameter is specified for this command, then SNMP is enabled or disabled for both IPv4 and IPv6.

**Mode** Global Configuration

**Examples** To enable SNMP on the device for both IPv4 and IPv6, use the commands:

```
awplus# configure terminal  
awplus(config)# snmp-server
```

To enable the SNMP agent for IPv4 on the device, use the commands:

```
awplus# configure terminal  
awplus(config)# snmp-server ip
```

To disable the SNMP agent for both IPv4 and IPv6 on the device, use the commands:

```
awplus# configure terminal  
awplus(config)# no snmp-server
```

To disable the SNMP agent for IPv4, use the commands:

```
awplus(config)# no snmp-server ipv4
```

**Related commands**

- show snmp-server
- show snmp-server community
- show snmp-server user
- snmp-server community
- snmp-server contact
- snmp-server enable trap
- snmp-server engineID local
- snmp-server group
- snmp-server host
- snmp-server location
- snmp-server view

# snmp-server community

**Overview** This command creates an SNMP community, optionally setting the access mode for the community. The default access mode is read only. If view is not specified, the community allows access to all the MIB objects. The SNMP communities are only valid for SNMPv1 and v2c and provide very limited security. Communities should not be used when operating SNMPv3.

The **no** variant of this command removes an SNMP community. The specified community must already exist on the device.

**Syntax** `snmp-server community <community-name> {view <view-name>|ro|rw}`  
`no snmp-server community <community-name> [{view <view-name>}]`

| Parameter        | Description  |
|------------------|--|
| <community-name> | Community name. The community name is a case sensitive string of up to 20 characters.              |
| view             | Configure SNMP view. If view is not specified, the community allows access to all the MIB objects. |
| <view-name>      | View name. The view name is a string up to 20 characters long and is case sensitive.               |
| ro               | Read-only community.   |
| rw               | Read-write community.  |

**Mode** Global Configuration

**Example** The following command creates an SNMP community called “public” with read only access to all MIB variables from any management station.

```
awplus# configure terminal  
awplus(config)# snmp-server community public ro
```

The following command removes an SNMP community called “public”

```
awplus# configure terminal  
awplus(config)# no snmp-server community public
```

**Related commands** [show snmp-server](#)  
[show snmp-server community](#)  
[snmp-server view](#)

# snmp-server contact

**Overview** This command sets the contact information for the system. The contact name is:

- displayed in the output of the [show system](#) command
- stored in the MIB object sysContact

The **no** variant of this command removes the contact information from the system.

**Syntax** `snmp-server contact <contact-info>`  
`no snmp-server contact`

| Parameter                         | Description   |
|-----------------------------------|---|
| <code>&lt;contact-info&gt;</code> | The contact information for the system, from 0 to 255 characters long. Valid characters are any printable character and spaces. |

**Mode** Global Configuration

**Example** To set the system contact information to "support@alliedtelesis.co.nz", use the command:

```
awplus# configure terminal
awplus(config)# snmp-server contact
support@alliedtelesis.co.nz
```

**Related commands** [show system](#)  
[snmp-server location](#)  
[snmp-server group](#)

# snmp-server enable trap

**Overview** Use this command to enable the switch to transmit the specified notifications (traps).

Note that the Environmental Monitoring traps defined in the AT-ENVMONv2-MIB are enabled by default.

Use the **no** variant of this command to disable the transmission of the specified notifications.

**Syntax** `snmp-server enable trap <trap-list>`  
`no snmp-server enable trap <trap-list>`

Depending on your device model, you can enable some or all of the traps in the following table:

| Parameter    | Description  |
|--------------|--|
| atmf         | AMF traps.   |
| atmflink     | AMF link traps.  |
| atmfnode     | AMF node traps.  |
| atmfrr       | AMF reboot-rolling traps.  |
| auth         | Authentication failure.  |
| bgp          | BGP traps.   |
| chassis      | Chassis traps.   |
| dhcpsnooping | DHCP snooping and ARP security traps. These notifications must also be set using the <b>ip dhcp snooping violation</b> command, and/or the arp security violation <b>arp security violation</b> command. |
| epsr         | EPSR traps.  |
| g8032        | G.8032 ERP traps.  |
| lldp         | Link Layer Discovery Protocol (LLDP) traps. These notifications must also be enabled using the <b>lldp notifications</b> command, and/or the <b>lldp med-notifications</b> command.                      |
| loopprot     | Loop Protection traps.   |
| mstp         | MSTP traps.  |
| nsm          | NSM traps.   |
| ospf         | OSPF traps.  |
| pim          | PIM traps.   |
| power-inline | Power-inline traps (Power Ethernet MIB RFC 3621).  |
| qsp          | QoS Storm Protection   |

| Parameter    | Description                             |
|--------------|---|
| rmon         | RMON traps.                             |
| thrash-limit | MAC address Thrash Limiting traps.      |
| vcs          | VCS traps.                              |
| vrrp         | Virtual Router Redundancy (VRRP) traps. |
| ufo          | Upstream Forwarding Only (UFO) traps.   |

**Default** By default, no notifications are generated.

**Mode** Global Configuration

**Usage notes** This command cannot be used to enable link status notifications globally. To enable link status notifications for particular interfaces, use the [snmp trap link-status](#) command.

To specify where notifications are sent, use the [snmp-server host](#) command.

Note that you can enable (or disable) multiple traps with a single command, by specifying a space-separated list of traps.

**Examples** To enable the device to send a notification if an AMF node changes its status, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap atmfnode
```

To enable the device to send MAC address Thrash Limiting traps, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap thrash-limit
```

To disable the device from sending MAC address Thrash Limiting traps, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server enable trap thrash-limit
```

**Related commands** [show snmp-server](#)  
[snmp trap link-status](#)  
[snmp-server host](#)

**Command changes** Version 5.4.7-2.1: **ufo** parameter added



# snmp-server engineID local

**Overview** Use this command to configure the SNMPv3 engine ID. The SNMPv3 engine ID is used to uniquely identify the SNMPv3 agent on a device when communicating with SNMP management clients. Once an SNMPv3 engine ID is assigned, this engine ID is permanently associated with the device until you change it.

Use the **no** variant of this command to set the user defined SNMPv3 engine ID to a system generated pseudo-random value by resetting the SNMPv3 engine. The **no snmp-server engineID local** command has the same effect as the **snmp-server engineID local default** command.

Note that the [snmp-server engineID local reset](#) command is used to force the system to generate a new engine ID when the current engine ID is also system generated.

**Syntax** `snmp-server engineID local {<engine-id>|default}`  
`no snmp-server engineID local`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;engine-id&gt;</code> | Specify SNMPv3 Engine ID value, a string of up to 27 characters.   |
| <code>default</code>           | Set SNMPv3 engine ID to a system generated value by resetting the SNMPv3 engine, provided the current engine ID is user defined. If the current engine ID is system generated, use the <a href="#">snmp-server engineID local reset</a> command to force the system to generate a new engine ID. |

**Mode** Global Configuration

**Usage notes** All devices must have a unique engine ID which is permanently set unless it is configured by the user.

**Example** To set the SNMPv3 engine ID to 800000cf030000cd123456, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local
800000cf030000cd123456
```

To set a user defined SNMPv3 engine ID back to a system generated value, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server engineID local
```

**Output** The following example shows the engine ID values after configuration:

```
awplus(config)#snmp-server engineid local asdgdfh231234d
awplus(config)#exit
awplus#show snmp-server

SNMP Server ..... Enabled
IP Protocol ..... IPv4
SNMPv3 Engine ID (configured name) ... asdgdfh231234d
SNMPv3 Engine ID (actual) ..... 0x80001f888029af52e149198483

awplus(config)#no snmp-server engineid local
awplus(config)#exit
awplus#show snmp-server

SNMP Server ..... Enabled
IP Protocol ..... IPv4
SNMPv3 Engine ID (configured name) ... Not set
SNMPv3 Engine ID (actual) ..... 0x80001f888029af52e149198483
```

**Related commands**

- [show snmp-server](#)
- [snmp-server engineID local reset](#)
- [snmp-server group](#)

# snmp-server engineID local reset

**Overview** Use this command to force the device to generate a new pseudo-random SNMPv3 engine ID by resetting the SNMPv3 engine. If the current engine ID is user defined, use the [snmp-server engineID local](#) command to set SNMPv3 engine ID to a system generated value.

**Syntax** `snmp-server engineID local reset`

**Mode** Global Configuration

**Example** To force the SNMPv3 engine ID to be reset to a system generated value, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local reset
```

**Related commands** [snmp-server engineID local](#)  
[show snmp-server](#)

# snmp-server group

**Overview** This command is used with SNMP version 3 only, and adds an SNMP group, optionally setting the security level and view access modes for the group. The security and access views defined for the group represent the minimum required of its users in order to gain access.

The **no** variant of this command deletes an SNMP group, and is used with SNMPv3 only. The group with the specified authentication/encryption parameters must already exist.

**Syntax** `snmp-server group <groupname> {auth|noauth|priv} [read <readname>|write <writename>|notify <notifyname>]`  
`no snmp-server group <groupname> {auth|noauth|priv}`

| Parameter    | Description   |
|--------------|---|
| <groupname>  | Group name. The group name is a string up to 20 characters long and is case sensitive.      |
| auth         | Authentication.   |
| noauth       | No authentication and no encryption.  |
| priv         | Authentication and encryption.  |
| read         | Configure read view.  |
| <readname>   | Read view name.   |
| write        | Configure write view.   |
| <writename>  | Write view name. The view name is a string up to 20 characters long and is case sensitive.  |
| notify       | Configure notify view.  |
| <notifyname> | Notify view name. The view name is a string up to 20 characters long and is case sensitive. |

**Mode** Global Configuration

**Examples** To add SNMP group, for ordinary users, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server group usergroup noauth read
useraccess write useraccess
```

To delete SNMP group `usergroup`, use the following commands

```
awplus# configure terminal
awplus(config)# no snmp-server group usergroup noauth
```

**Related  
commands** `snmp-server`  
`show snmp-server`  
`show snmp-server group`  
`show snmp-server user`

# snmp-server host

**Overview** This command specifies an SNMP trap host destination to which Trap or Inform messages generated by the device are sent.

For SNMP version 1 and 2c you must specify the community name parameter. For SNMP version 3, specify the authentication/encryption parameters and the user name. If the version is not specified, the default is SNMP version 1. Inform messages can be sent instead of traps for SNMP version 2c and 3.

Use the **no** variant of this command to remove an SNMP trap host. The trap host must already exist.

The trap host is uniquely identified by:

- host IP address (IPv4 or IPv6),
- inform or trap messages,
- community name (SNMPv1 or SNMP v2c) or the authentication/encryption parameters and user name (SNMP v3).

**Syntax**

```
snmp-server host {<ipv4-address>/<ipv6-address>} [traps]
[version 1] <community-name>]

snmp-server host {<ipv4-address>/<ipv6-address>}
[informs|traps] version 2c <community-name>

snmp-server host {<ipv4-address>/<ipv6-address>}
[informs|traps] version 3 {auth|noauth|priv} <user-name>

no snmp-server host {<ipv4-address>/<ipv6-address>} [traps]
[version 1] <community-name>

no snmp-server host {<ipv4-address>/<ipv6-address>}
[informs|traps] version 2c <community-name>

no snmp-server host {<ipv4-address>/<ipv6-address>}
[informs|traps] version 3 {auth|noauth|priv} <user-name>
```

| Parameter      | Description   |
|----------------|---|
| <ipv4-address> | IPv4 trap host address in the format A . B . C . D, for example, 192 . 0 . 2 . 2.             |
| <ipv6-address> | IPv6 trap host address in the format x : x : : x : x for example, 2001 : db8 : : 8a2e : 7334. |
| informs        | Send Inform messages to this host.  |
| traps          | Send Trap messages to this host (default).  |
| version        | SNMP version to use for notification messages. Default: version 1.                            |
| 1              | Use SNMPv1 (default).   |
| 2c             | Use SNMPv2c.  |
| 3              | Use SNMPv3.   |

| Parameter        | Description                           |
|------------------|---------------------------------------|
| auth             | Authentication.                       |
| noauth           | No authentication.                    |
| priv             | Encryption.                           |
| <community-name> | The SNMPv1 or SNMPv2c community name. |
| <user-name>      | SNMPv3 user name.                     |

**Mode** Global Configuration

**Examples** To configure the device to send generated traps to the IPv4 host destination 192.0.2.5 with the SNMPv2c community name public, use the following command:

```
awplus# configure terminal
awplus(config)# snmp-server host version 2c public192.0.2.5
```

To configure the device to send generated traps to the IPv6 host destination 2001:db8::8a2e:7334 with the SNMPv2c community name private, use the following command:

```
awplus# configure terminal
awplus(config)# snmp-server host version 2c
private2001:db8::8a2e:7334
```

To remove a configured trap host of 192.0.2.5 with the SNMPv2c community name public, use the following command:

```
awplus# configure terminal
awplus(config)# no snmp-server host version 2c public192.0.2.5
```

**Related commands**

- [snmp trap link-status](#)
- [snmp-server enable trap](#)
- [snmp-server view](#)

# snmp-server legacy-ifadminstatus

**Overview** Use this command to set the ifAdminStatus to reflect the operational state of the interface, rather than the administrative state.

The **no** variant of this command sets the ifAdminStatus to reflect the administrative state of the interface.

**Syntax** `snmp-server legacy-ifadminstatus`  
`no snmp-server legacy-ifadminstatus`

**Default** Legacy ifAdminStatus is turned off by default, so by default the SNMP ifAdminStatus reflects the administrative state of the interface.

**Mode** Global Configuration

**Usage notes** Note that if you enable Legacy ifAdminStatus, the ifAdminStatus will report a link's status as Down when the link has been blocked by a process such as loop protection.

**Example** To turn on Legacy ifAdminStatus, use the command:

```
awplus#snmp-server legacy-ifadminstatus
```

**Related commands** [show interface](#)



# snmp-server location

**Overview** This command sets the location of the system. The location is:

- displayed in the output of the [show system](#) command
- stored in the MIB object sysLocation

The **no** variant of this command removes the configured location from the system.

**Syntax** `snmp-server location <location-name>`  
`no snmp-server location`

| Parameter                          | Description   |
|------------------------------------|---|
| <code>&lt;location-name&gt;</code> | The location of the system, from 0 to 255 characters long. Valid characters are any printable character and spaces. |

**Mode** Global Configuration

**Example** To set the location to “server room 523”, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server location server room 523
```

**Related commands** [show snmp-server](#)  
[show system](#)  
[snmp-server contact](#)

# snmp-server source-interface

**Overview** Use this command to specify the originating interface for SNMP traps or informs. An interface specified by this command must already have an IP address assigned to it.

Use the **no** variant of this command to reset the interface to its default value (the originating egress interface).

**Syntax** `snmp-server source-interface {traps|informs} <interface-name>`  
`no snmp-server source-interface {traps|informs}`

| Parameter        | Description  |
|------------------|--|
| traps            | SNMP traps.  |
| informs          | SNMP informs.  |
| <interface-name> | Interface name (must already have an IP address assigned). |

**Default** By default, the source interface is the originating egress interface of the traps and informs messages.

**Mode** Global Configuration

**Usage notes** An SNMP trap or inform message that is sent from an SNMP server carries the notification IP address of its originating interface. Use this command to assign this interface.

**Example** The following commands set vlan1 to be the interface whose IP address is used as the originating address in SNMP informs packets.

```
awplus# configure terminal
awplus(config)# snmp-server source-interface informs vlan1
```

The following commands reset the originating source interface for SNMP trap messages to be the default interface (the originating egress interface):

```
awplus# configure terminal
awplus(config)# no snmp-server source-interface traps
```

**Validation Commands** `show running-config`

# snmp-server startup-trap-delay

**Overview** Use this command to set the time in seconds after following completion of the device startup sequence before the device sends any SNMP traps (or SNMP notifications).

Use the no variant of this command to restore the default startup delay of 30 seconds.

**Syntax** `snmp-server startup-trap-delay <delay-time>`  
`no snmp-server startup-trap-delay`

| Parameter                       | Description   |
|---------------------------------|---|
| <code>&lt;delay-time&gt;</code> | Specify an SNMP trap delay time in seconds in the range of 30 to 600 seconds. |

**Default** The SNMP server trap delay time is 30 seconds. The no variant restores the default.

**Mode** Global Configuration

**Example** To delay the device sending SNMP traps until 60 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server startup-trap-delay 60
```

To restore the sending of SNMP traps to the default of 30 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server startup-trap-delay
```

**Validation Commands** `show snmp-server`

# snmp-server user

**Overview** Use this command to create or move users as members of specified groups. This command is used with SNMPv3 only.

The **no** variant of this command removes an SNMPv3 user. The specified user must already exist.

**Syntax** `snmp-server user <username> <groupname> [encrypted] [auth {md5|sha} <auth-password>] [priv {des|aes} <privacy-password>]`  
`no snmp-server user <username>`

| Parameter                             | Description   |
|---------------------------------------|---|
| <code>&lt;username&gt;</code>         | User name. The user name is a string up to 20 characters long and is case sensitive.                |
| <code>&lt;groupname&gt;</code>        | Group name. The group name is a string up to 20 characters long and is case sensitive.              |
| <code>encrypted</code>                | Use the encrypted parameter when you want to enter encrypted passwords.                             |
| <code>auth</code>                     | Authentication protocol.  |
| <code>md5</code>                      | MD5 Message Digest Algorithms.  |
| <code>sha</code>                      | SHA Secure Hash Algorithm.  |
| <code>&lt;auth-password&gt;</code>    | Authentication password. The password is a string of 8 to 20 characters long and is case sensitive. |
| <code>priv</code>                     | Privacy protocol.   |
| <code>des</code>                      | DES: Data Encryption Standard.  |
| <code>aes</code>                      | AES: Advanced Encryption Standards.   |
| <code>&lt;privacy-password&gt;</code> | Privacy password. The password is a string of 8 to 20 characters long and is case sensitive.        |

**Mode** Global Configuration

**Usage notes** Additionally this command provides the option of selecting an authentication protocol and (where appropriate) an associated password. Similarly, options are offered for selecting a privacy protocol and password.

- Note that each SNMP user must be configured on both the manager and agent entities. Where passwords are used, these passwords must be the same for both entities.
- Use the **encrypted** parameter when you want to enter already encrypted passwords in encrypted form as displayed in the running and startup configs stored on the device. For example, you may need to move a user from one group to another group and keep the same passwords for the user instead of removing the user to apply new passwords.

- User passwords are entered using plaintext without the **encrypted** parameter and are encrypted according to the authentication and privacy protocols selected.
- User passwords are viewed as encrypted passwords in running and startup configs shown from **show running-config** and **show startup-config** commands respectively. Copy and paste encrypted passwords from running-configs or startup-configs to avoid entry errors.

**Examples** To add SNMP user authuser as a member of group “usergroup”, with authentication protocol MD5, authentication password “Authpass”, privacy protocol AES and privacy password “Privpass”, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server user authuser usergroup auth md5
Authpass priv aes Privpass
```

Validate the user is assigned to the group using the **show snmp-server user** command:

```
awplus#show snmp-server user
Name                Group name          Auth                Privacy
-----            -
authuser            usergroup           md5                 aes
```

To enter existing SNMP user “authuser” with existing passwords as a member of group “newusergroup” with authentication protocol MD5 with the encrypted authentication password 0x1c74b9c22118291b0ce0cd883f8dab6b74, and privacy protocol AES with the encrypted privacy password 0x0e0133db5453ebd03822b004eeacb6608f, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server user authuser newusergroup
encrypted auth md5 0x1c74b9c22118291b0ce0cd883f8dab6b74 priv
aes 0x0e0133db5453ebd03822b004eeacb6608f
```

**NOTE:** Copy and paste the encrypted passwords from the **running-config** or the **startup-config** displayed, using the **show running-config** and **show startup-config** commands respectively, into the command line to avoid key stroke errors issuing this command.

Validate the user has been moved from the first group using the **show snmp-server user** command:

```
awplus#show snmp-server user
Name                Group name          Auth                Privacy
-----            -
authuser            newusergroup        md5                 aes
```

To delete SNMP user “authuser”, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server user authuser
```

**Related  
commands** [show snmp-server user](#)  
[snmp-server view](#)

# snmp-server view

**Overview** Use this command to create an SNMP view that specifies a sub-tree of the MIB. Further sub-trees can then be added by specifying a new OID to an existing view. Views can be used in SNMP communities or groups to control the remote manager's access.

**NOTE:** The object identifier must be specified in a sequence of integers separated by decimal points.

The **no** variant of this command removes the specified view on the device. The view must already exist.

**Syntax** `snmp-server view <view-name> <mib-name> {included|excluded}`  
`no snmp-server view <view-name>`

| Parameter   | Description   |
|-------------|---|
| <view-name> | SNMP server view name.<br>The view name is a string up to 20 characters long and is case sensitive. |
| <mib-name>  | Object identifier of the MIB.   |
| included    | Include this OID in the view.   |
| excluded    | Exclude this OID in the view.   |

**Mode** Global Configuration

**Examples** The following command creates a view called "loc" that includes the system location MIB sub-tree.

```
awplus(config)# snmp-server view loc 1.3.6.1.2.1.1.6.0 included
```

To remove the view "loc" use the following command

```
awplus(config)# no snmp-server view loc
```

**Related commands** [show snmp-server view](#)  
[snmp-server community](#)

# undebbug snmp

**Overview** This command applies the functionality of the no `debug snmp` command.



# 24

# Mail (SMTP) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure mail. The mail feature uses Simple Mail Transfer Protocol (SMTP) to transfer mail from an internal email client operating within the AlliedWare Plus device. This feature is typically used to email event notifications to an external email server from the AlliedWare Plus device.

For information on using the mail feature, see the [Mail \(SMTP\) Feature Overview and Configuration Guide](#).

- Command List**
- “[debug mail](#)” on page 1098
  - “[delete mail](#)” on page 1099
  - “[mail](#)” on page 1100
  - “[mail from](#)” on page 1102
  - “[mail smtpserver](#)” on page 1103
  - “[mail smtpserver authentication](#)” on page 1104
  - “[mail smtpserver port](#)” on page 1106
  - “[show counter mail](#)” on page 1108
  - “[show mail](#)” on page 1109
  - “[undebug mail](#)” on page 1110

# debug mail

**Overview** This command turns on debugging for sending emails.  
The **no** variant of this command turns off debugging for sending emails.

**Syntax** debug mail  
no debug mail

**Mode** Privileged Exec

**Examples** To turn on debugging for sending emails, use the command:

```
awplus# debug mail
```

To turn off debugging for sending emails, use the command:

```
awplus# no debug mail
```

**Related commands**

- delete mail
- mail
- mail from
- mail smtpserver
- show counter mail
- show mail
- undebug mail

# delete mail

**Overview** This command deletes mail from the queue.

You need the *mail-id* from the **show mail** command output to delete specific emails, or use the **all** parameter to clear all messages in the queue completely.

**Syntax** `delete mail [mail-id <mail-id>|all]`

| Parameter | Description   |
|-----------|---|
| mail-id   | Deletes a single mail from the mail queue.  |
|           | <mail-id> A unique mail ID number. Use the <a href="#">show mail</a> command to display this for an item of mail. |
| all       | Delete all the mail in the queue.   |

**Mode** Privileged Exec

**Examples** To delete the unique mail item "20060912142356.1234" from the queue, use the command:

```
awplus# delete mail 20060912142356.1234
```

To delete all mail from the queue, use the command:

```
awplus# delete mail all
```

**Related commands**

- [debug mail](#)
- [mail](#)
- [mail from](#)
- [mail smtpserver](#)
- [show mail](#)

# mail

**Overview** This command sends an email using the SMTP protocol. If you specify a file the text inside the file is sent in the message body.

If you do not specify the **to**, **file**, or **subject** parameters, the CLI prompts you for the missing information.

Before you can send mail using this command, you must specify the sending email address using the [mail from](#) command and a mail server using the [mail smtpserver](#) command.

**Syntax** mail [to <to>] [subject <subject>] [file <filename>]

| Parameter | Description   |
|-----------|---|
| to        | The email recipient.<br><br><to> Email address.   |
| subject   | Description of the subject of this email. Use quote marks when the subject text contains spaces.<br><br><subject> String. |
| file      | File to insert as text into the message body.<br><br><filename> String.   |

**Mode** Privileged Exec

**Usage notes** When you use the **mail** command you can use parameter substitutions in the subject field. The following table lists the parameters that can be substituted and their descriptions:

| Parameter            | Description  |
|----------------------|--|
| <%N>                 | When this parameter is specified, the %N is replaced by the host name of your device.                                  |
| <%S>                 | When this parameter is specified, the %S is replaced by the serial number of your device.                              |
| <%D><br><%L><br><%T> | When any of these parameters is specified, they are replaced by the current date and time (local time) on your device. |
| <%U>                 | When this parameter is specified, the %U is replaced by the current date and time (UTC time) on your device.           |

**NOTE:** If no local time is configured, it will use UTC.

**Examples** To send an email to "admin@example.com" with the subject "test email" and with the message body inserted from the file "test.conf", use the command:

```
awplus# mail to admin@example.com subject "test email" filename  
test.conf
```

To send an email using parameter substitutions for the host name, serial number and date, use the commands:

```
awplus# mail to admin@example.com subject "Sending email from  
Hostname:%N Serial Number:%S Date:%T"
```

**Related  
commands**

[debug mail](#)

[delete mail](#)

[mail from](#)

[mail smtpserver](#)

[mail smtpserver authentication](#)

[mail smtpserver port](#)

[show counter mail](#)

[show mail](#)

# mail from

**Overview** This command sets an email address as the sender. You must specify a sending email address with this command before you can send email.

Use the **no** variant of this command to remove the “mail from” address.

**Syntax** mail from <from>  
no mail from

| Parameter | Description  |
|-----------|--|
| <from>    | The email address that the mail is sent from (also known as the hostname). |

**Mode** Global Configuration

**Example** To set up your email address as the sender “kaji@nerv.com”, use the command:

```
awplus(config)# mail from kaji@nerv.com
```

**Related commands**

- debug mail
- delete mail
- mail
- mail smtpserver
- show counter mail
- show mail
- undebug mail

# mail smtpserver

**Overview** This command specifies the IP address or domain name of the SMTP server that your device sends email to. You must specify a mail server with this command before you can send email.

Use the **no** variant of this command to remove the configured mail server.

**Syntax** mail smtpserver {<ip-address>|<name>}  
no mail smtpserver

| Parameter    | Description   |
|--------------|---|
| <ip-address> | Internet Protocol (IP) address for the mail server.                   |
| <name>       | Domain name (FQDN) for the mail server (also known as the host name). |

**Mode** Global Configuration

**Usage notes** If you specify the server by specifying its domain name, you must also ensure that the DNS client on your device is enabled. It is enabled by default but if it has been disabled, you can re-enable it by using the [ip domain-lookup](#) command.

**Examples** To specify a mail server at "192.168.0.1", use the command:

```
awplus(config)# mail smtpserver 192.168.0.1
```

To specify a mail server that has a host name of "smtp.example.com", use the command:

```
awplus(config)# mail smtpserver smtp.example.com
```

To remove the configured mail server, use the command:

```
awplus(config)# no mail smtpserver
```

**Related commands**

- [debug mail](#)
- [delete mail](#)
- [mail](#)
- [mail from](#)
- [show counter mail](#)
- [show mail](#)

# mail smtpserver authentication

**Overview** Use this command to configure SMTP mail server authentication.

Use the **no** variant of this command to remove the configured SMTP mail server authentication.

**Syntax** mail smtpserver authentication {crammd5|login|plain} username <username> password [8] <password>  
no mail smtpserver authentication

| Parameter  | Description  |
|------------|--|
| crammd5    | This is a Challenge Request Authentication Mechanism based on the HMAC-MD5 mechanism and is the most secure option.  |
| login      | A BASE64 encryption method   |
| plain      | A BASE64 encryption method   |
| <username> | Registered user name   |
| 8          | The registered user password is presented in an already encrypted format. This is how the running configuration stores the plain text password and is not for general use. |
| <password> | Registered user password   |

**Default** No authentication option is set by default.

**Mode** Global Configuration

**Usage notes** You cannot change the IP address or Domain Name of the SMTP server if authentication is configured. If you attempt to change it when authentication is configured, the following error message is displayed:

```
% Error: authentication configuration still exists
```

**Examples** To configure the SMTP mail server authentication to crammd5, use the commands:

```
awplus# configure terminal  
awplus(config)# mail smtpserver authentication crammd5 username  
admin password unguessablePassword
```

To remove SMTP mail server authentication, use the commands:

```
awplus# configure terminal  
awplus(config)# no mail smtpserver authentication
```



**Output** Figure 24-1: Example output from **show mail**:

```
awplus#show mail
Mail Settings
-----
State                : Alive
SMTP Server          : 1.2.3.4
Host Name             : admin@example.com
Authentication       : crammd5
Username              : admin
Debug                 : Disabled

awplus#show running-config
!
mail smtpserver authentication plain username admin password 8
aF0a9pkjbmXGfl6TlSk/GakeIK5tMYN6LqMYT8Ia2qw=
!
```

**Related  
commands**

[debug mail](#)  
[delete mail](#)  
[mail](#)  
[mail from](#)  
[mail smtpserver](#)  
[mail smtpserver port](#)  
[show counter mail](#)  
[show mail](#)

**Command  
changes**

Version 5.4.8-1.1: command added

# mail smtpserver port

**Overview** Use this command to configure the SMTP mail client/server communication port. Use the **no** variant of this command to remove the configured port and set it back to the default port 25.

**Syntax** mail smtpserver port <port>  
no mail smtpserver port

| Parameter | Description                           |
|-----------|---------------------------------------|
| <port>    | Port number from the range 1 to 65535 |

**Default** Port 25 is the default port.

**Mode** Global Configuration

**Examples** To configure the mail server communication over port 587, use the commands:

```
awplus# configure terminal  
awplus(config)# mail smtpserver port 587
```

To remove the configured port and set it back to the default port 25, use the commands:

```
awplus# configure terminal  
awplus(config)# no mail smtpserver port
```

**Output** Figure 24-2: Example output from **show mail**:

```
awplus#show mail  
Mail Settings  
-----  
State : Alive  
SMTP Server : 10.24.165.4  
Host Name : admin@example.com  
Authentication : plain  
Username : admin  
Port : 587  
Debug : Disabled  
  
awplus#show running-config  
!  
mail smtpserver port 587  
!
```

**Related commands** [debug mail](#)  
[delete mail](#)  
[mail](#)

mail from  
mail smtpserver  
mail smtpserver authentication  
show counter mail  
show mail

**Command changes** Version 5.4.8-1.1: command added

# show counter mail

**Overview** This command displays the mail counters.

**Syntax** show counter mail

**Mode** User Exec and Privileged Exec

**Example** To show the emails in the queue use the command:

```
awplus# show counter mail
```

**Output** Figure 24-3: Example output from the **show counter mail** command

```
Mail Client (SMTP) counters
Mails Sent           ..... 2
Mails Sent Fails     ..... 1
```

**Table 1:** Parameters in the output of the **show counter mail** command

| Parameter        | Description   |
|------------------|---|
| Mails Sent       | The number of emails sent successfully since the last device restart.         |
| Mails Sent Fails | The number of emails the device failed to send since the last device restart. |

**Related commands**

- [debug mail](#)
- [delete mail](#)
- [mail](#)
- [mail from](#)
- [show mail](#)

# show mail

**Overview** This command displays the emails in the queue.

**Syntax** show mail

**Mode** Privileged Exec

**Example** To display the emails in the queue use the command:

```
awplus# show mail
```

**Output** Figure 24-4: Example output from the **show mail** command:

```
awplus#show mail
Mail Settings
-----
State                : Alive
SMTP Server          : example.net
Host Name             : test@example.com
Debug                 : Enabled

Messages
-----
To                   : rei@nerv.com
Subject              : The WAN is down
Message-ID           : 20180615121150.8663

To                   : rei@nerv.com
Subject              : WAN is not connecting in the lab
Message-ID           : 20180614142502.19308

To                   : rei@nerv.com
Subject              : The LAN is not functioning
Message-ID           : 20180614141911.29709
```

**Related commands**

- [delete mail](#)
- [mail](#)
- [mail from](#)
- [mail smtpserver](#)
- [show counter mail](#)
- [undebug mail](#)

# undebug mail

**Overview** This command applies the functionality of the no `debug mail` command.

# 25

# Secure Shell (SSH) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure Secure Shell (SSH). For more information, see the [SSH Feature Overview and Configuration Guide](#).

- Command List**
- “[banner login \(SSH\)](#)” on page 1113
  - “[clear ssh](#)” on page 1114
  - “[crypto key destroy hostkey](#)” on page 1115
  - “[crypto key destroy userkey](#)” on page 1116
  - “[crypto key generate hostkey](#)” on page 1117
  - “[crypto key generate userkey](#)” on page 1119
  - “[crypto key pubkey-chain userkey](#)” on page 1120
  - “[debug ssh server](#)” on page 1122
  - “[service ssh](#)” on page 1123
  - “[show banner login](#)” on page 1125
  - “[show crypto key hostkey](#)” on page 1126
  - “[show crypto key pubkey-chain userkey](#)” on page 1128
  - “[show crypto key userkey](#)” on page 1129
  - “[show running-config ssh](#)” on page 1130
  - “[show ssh](#)” on page 1132
  - “[show ssh server](#)” on page 1134
  - “[show ssh server allow-users](#)” on page 1136
  - “[show ssh server deny-users](#)” on page 1137
  - “[ssh server](#)” on page 1138

- [“ssh server allow-users”](#) on page 1140
- [“ssh server authentication”](#) on page 1142
- [“ssh server deny-users”](#) on page 1144
- [“ssh server max-auth-tries”](#) on page 1146
- [“ssh server resolve-host”](#) on page 1147
- [“ssh server scp”](#) on page 1148
- [“ssh server sftp”](#) on page 1149
- [“undebbug ssh server”](#) on page 1150



# banner login (SSH)

**Overview** This command configures a login banner on the SSH server. This displays a message on the remote terminal of the SSH client before the login prompt. SSH client version 1 does not support this banner.

To add a banner, first enter the command **banner login**, and hit [Enter]. Write your message. You can use any character and spaces. Use Ctrl+D at the end of your message to save the text and re-enter the normal command line mode.

The banner message is preserved if the device restarts.

The **no** variant of this command deletes the login banner from the device.

**Syntax** banner login  
no banner login

**Default** No banner is defined by default.

**Mode** Global Configuration

**Examples** To set a login banner message, use the commands:

```
awplus# configure terminal  
awplus(config)# banner login
```

The screen will prompt you to enter the message:

Type CNTL/D to finish.

... banner message comes here ...

Enter the message. Use Ctrl+D to finish, like this:

```
^D  
awplus(config)#
```

To remove the login banner message, use the commands:

```
awplus# configure terminal  
awplus(config)# no banner login
```

**Related commands** [show banner login](#)

# clear ssh

**Overview** This command deletes Secure Shell sessions currently active on the device. This includes both incoming and outgoing sessions. The deleted sessions are closed. You can only delete an SSH session if you are a system manager or the user who initiated the session. If **all** is specified then all active SSH sessions are deleted.

**Syntax** `clear ssh {<1-65535>|all}`

| Parameters | Description  |
|------------|--|
| <1-65535>  | Specify a session ID in the range 1 to 65535 to delete a specific session. |
| all        | Delete all SSH sessions.   |

**Mode** Privileged Exec

**Examples** To stop the current SSH session 123, use the command:

```
awplus# clear ssh 123
```

To stop all SSH sessions active on the device, use the command:

```
awplus# clear ssh all
```

**Related commands** [service ssh](#)

# crypto key destroy hostkey

**Overview** This command deletes the existing public and private keys of the SSH server.

When you enable the SSH server, the server automatically generates an SSHv2 host key pair (public and private keys), using RSA with 1024-bit key generation. If you need a key with different parameters than this, you can use the [crypto key generate hostkey](#) command to generate that key before you enable the SSH server.

**Syntax** `crypto key destroy hostkey {dsa|ecdsa|rsa|rsa1}`

| Parameters         | Description  |
|--------------------|--|
| <code>dsa</code>   | Deletes the existing DSA public and private keys.  |
| <code>ecdsa</code> | Deletes the existing ECDSA public and private keys.  |
| <code>rsa</code>   | Deletes the existing RSA public and private keys configured for SSH version 2 connections. |
| <code>rsa1</code>  | Deletes the existing RSA public and private keys configured for SSH version 1 connections. |

**Mode** Global Configuration

**Example** To destroy the RSA host key used for SSH version 2 connections, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy hostkey rsa
```

**Related commands** [crypto key generate hostkey](#)  
[service ssh](#)

# crypto key destroy userkey

**Overview** This command destroys the existing public and private keys of an SSH user configured on the device.

**Syntax** `crypto key destroy userkey <username> {dsa|rsa|rsa1}`

| Parameters                    | Description  |
|-------------------------------|--|
| <code>&lt;username&gt;</code> | 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. |
| <code>dsa</code>              | Deletes the existing DSA userkey.  |
| <code>rsa</code>              | Deletes the existing RSA userkey configured for SSH version 2 connections.   |
| <code>rsa1</code>             | Deletes the existing RSA userkey for SSH version 1 connections.  |

**Mode** Global Configuration

**Example** To destroy the RSA user key for the SSH user `remoteuser`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy userkey remoteuser rsa
```

**Related commands**

- [crypto key generate hostkey](#)
- [show ssh](#)
- [show crypto key hostkey](#)

# crypto key generate hostkey

**Overview** This command generates public and private keys for the SSH server.

When you enable the SSH server, the server automatically generates an SSHv2 host key pair (public and private keys), using RSA with 1024-bit key generation.

If you need a key with different parameters than this, you can use this command to generate that key before you enable the SSH server. If a host key exists with the same cryptography algorithm, this command replaces the old host key with the new key.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

**Syntax** `crypto key generate hostkey {dsa} [<768-1024>]`  
`crypto key generate hostkey {rsa|rsa1} [<768-32768>]`  
`crypto key generate hostkey {ecdsa} [<256/384>]`

| Parameters  | Description   |
|-------------|---|
| dsa         | Creates a DSA hostkey. Both SSH version 1 and 2 connections can use the DSA hostkey.      |
| rsa         | Creates an RSA hostkey for SSH version 2 connections.                                     |
| rsa1        | Creates an RSA hostkey for SSH version 1 connections.                                     |
| ecdsa       | Creates an ECDSA hostkey. Both SSH version 1 and 2 connections can use the ECDSA hostkey. |
| <768-32768> | The length in bits of the generated key. The default is 1024 bits.                        |
| <256/384>   | The ECDSA key size in bits. The default is 256, but it can be set to 384.                 |

**Default** The default key length for RSA and DSA is 1024 bits.

The default key size for ECDSA is 256 bits.

**Mode** Global Configuration

**Examples** To generate an RSA host key for SSH version 2 connections that is 2048 bits in length, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa 2048
```

To generate a DSA host key, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate dsa
```

To generate an ECDSA host key with an elliptic curve size of 384 bits, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# crypto key generate ecdsa 384
```

**Related  
commands**

[crypto key destroy hostkey](#)

[service ssh](#)

[show crypto key hostkey](#)

# crypto key generate userkey

**Overview** This command generates public and private keys for an SSH user using either an RSA or DSA cryptography algorithm. To use public key authentication, copy the public key of the user onto the remote SSH server.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

**Syntax** `crypto key generate userkey <username> {dsa} [<768-1024>]`  
`crypto key generate userkey <username> {rsa|rsa1} [<768-32768>]`  
`crypto key generate userkey <username> {ecdsa} [<256/384>]`

| Parameters  | Description  |
|-------------|--|
| <username>  | Name of the user that the user key is generated for. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. |
| dsa         | Creates a DSA userkey. Both SSH version 1 and 2 connections can use a key created with this command.   |
| rsa         | Creates an RSA userkey for SSH version 2 connections.  |
| rsa1        | Creates an RSA userkey for SSH version 1 connections.  |
| ecdsa       | Creates an ECDSA hostkey. Both SSH version 1 and 2 connections can use the ECDSA hostkey.  |
| <768-32768> | The length in bits of the generated key. The default is 1024 bits.   |
| <256/384>   | The ECDSA key size in bits. The default is 256, but it can be set to 384.  |

**Mode** Global Configuration

**Examples** To generate a 2048-bits RSA user key for SSH version 2 connections for the user "bob", use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey bob rsa 2048
```

To generate a DSA user key for the user "lapo", use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey lapo dsa
```

**Related commands** [crypto key pubkey-chain userkey](#)  
[show crypto key userkey](#)

# crypto key pubkey-chain userkey

**Overview** This command adds a public key for an SSH user on the SSH server. This allows the SSH server to support public key authentication for the SSH user. When configured, the SSH user can access the SSH server without providing a password from the remote host.

The **no** variant of this command removes a public key for the specified SSH user that has been added to the public key chain. When a SSH user's public key is removed, the SSH user can no longer login using public key authentication.

**Syntax** `crypto key pubkey-chain userkey <username> [<filename>]`  
`no crypto key pubkey-chain userkey <username> <1-65535>`

| Parameters | Description  |
|------------|--|
| <username> | Name of the user that the SSH server associates the key with. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.<br>Default: no default |
| <filename> | Filename of a key saved in flash. Valid characters are any printable character. You can add a key as a hexadecimal string directly into the terminal if you do not specify a filename.                                   |
| <1-65535>  | The key ID number of the user's key. Specify the key ID to delete a key.   |

**Mode** Global Configuration

**Usage notes** You should import the public key file from the client node. The device can read the data from a file on the flash or user terminal.

Or you can add a key as text into the terminal. To add a key as text into the terminal, first enter the command **crypto key pubkey-chain userkey <username>**, and hit [Enter]. Enter the key as text. Note that the key you enter as text must be a valid SSH RSA key, not random ASCII text. Use [Ctrl]+D after entering it to save the text and re-enter the normal command line mode.

Note you can generate a valid SSH RSA key on the device first using the **crypto key generate host rsa** command. View the SSH RSA key generated on the device using the **show crypto hostkey rsa** command. Copy and paste the displayed SSH RSA key after entering the **crypto key pubkey-chain userkey <username>** command. Use [Ctrl]+D after entering it to save it.



**Examples** To generate a valid SSH RSA key on the device and add the key, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto key generate host rsa
awplus(config)# exit

awplus# show crypto key hostkey
rsaAAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fcOw1TStpb9J20bWluh
nUC768EoWhyPW6FZ2t5360O5M29EpKBmGq1kQaz5V0mU9IQe66+5YyD4UxOKSD
tTI+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16+6NvNbk+h+c/pqGDijj4SvfZZfe
ITzvvyZW4/I4pbN8=

awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey joeType CNTRL/D
to
finish:AAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fcOw1TStpb9J20b
WluhnUC768EoWhyPW6FZ2t5360O5M29EpKBmGq1kQaz5V0mU9IQe66+5YyD4Ux
OKSDtTI+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16+6NvNbk+h+c/pqGDijj4Svf
ZZfeITzvvyZW4/I4pbN8=control-D

awplus(config)#
```

To add a public key for the user `graydon` from the file `key.pub`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey graydon key.pub
```

To add a public key for the user `tamara` from the terminal, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey tamara
```

and enter the key. Use Ctrl+D to finish.

To remove the first key entry from the public key chain of the user `john`, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto key pubkey-chain userkey john 1
```

**Related commands** [show crypto key pubkey-chain userkey](#)

# debug ssh server

**Overview** This command enables the SSH server debugging facility. When enabled, the SSH server sends diagnostic messages to the system log. To display the debugging messages on the terminal, use the **terminal monitor** command.

The **no** variant of this command disables the SSH server debugging facility. This stops the SSH server from generating diagnostic debugging messages.

**Syntax** `debug ssh server [brief|full]`  
`no debug ssh server`

| Parameter | Description               |
|-----------|---------------------------|
| brief     | Enables brief debug mode. |
| full      | Enables full debug mode.  |

**Default** SSH server debugging is disabled by default.

**Mode** Privileged Exec and Global Configuration

**Examples** To start SSH server debugging, use the command:

```
awplus# debug ssh server
```

To start SSH server debugging with extended output, use the command:

```
awplus# debug ssh server full
```

To disable SSH server debugging, use the command:

```
awplus# no debug ssh server
```

**Related commands** [show ssh server](#)  
[undebug ssh server](#)

# service ssh

**Overview** Use this command to enable the Secure Shell server on the device. Once enabled, connections coming from SSH clients are accepted.

When you enable the SSH server, the server automatically generates an SSHv2 host key pair (public and private keys), using RSA with 1024-bit key generation. If you need a key with different parameters than this, you can use the [crypto key generate hostkey](#) command to generate that key before you enable the SSH server.

Use the **no** variant of this command disables the Secure Shell server. When the Secure Shell server is disabled, connections from SSH, SCP, and SFTP clients are not accepted. This command does not affect existing SSH sessions. To terminate existing sessions, use the [clear ssh](#) command.

**Syntax** `service ssh [ip|ipv6]`  
`no service ssh [ip|ipv6]`

**Default** The Secure Shell server is disabled by default. Both IPv4 and IPv6 Secure Shell server are enabled when you issue **service ssh** without specifying the optional **ip** or **ipv6** parameters.

**Mode** Global Configuration

**Examples** To enable both the IPv4 and the IPv6 Secure Shell server, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh
```

To enable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ip
```

To enable the IPv6 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ipv6
```

To disable both the IPv4 and the IPv6 Secure Shell server, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh
```

To disable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ip
```

To disable the IPv6 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ipv6
```

**Related commands**

- crypto key generate hostkey
- show running-config ssh
- show ssh server
- ssh server allow-users
- ssh server deny-users

# show banner login

**Overview** This command displays the banner message configured on the device. The banner message is displayed to the remote user before user authentication starts.

**Syntax** `show banner login`

**Mode** User Exec, Privileged Exec, Global Configuration, Interface Configuration, Line Configuration

**Example** To display the current login banner message, use the command:

```
awplus# show banner login
```

**Related commands** [banner login \(SSH\)](#)

# show crypto key hostkey

**Overview** This command displays the public keys generated on the device for the SSH server.

When you enable the SSH server, the server automatically generates an SSHv2 host key pair (public and private keys), using RSA with 1024-bit key generation. If you need a key with different parameters than this, you can use the [crypto key generate hostkey](#) command to generate that key before you enable the SSH server.

The private key remains on the device secretly. The public key is copied to SSH clients to identify the server. This command displays the public key.

**Syntax** `show crypto key hostkey [dsa|ecdsa|rsa|rsa1]`

| Parameter | Description  |
|-----------|--|
| dsa       | Displays the DSA algorithm public key. Both SSH version 1 and 2 connections can use the DSA hostkey      |
| ecdsa     | Displays the ECDSA algorithm public key. Both SSH version 1 and 2 connections can use the ECDSA hostkey. |
| rsa       | Displays the RSA algorithm public key for SSH version 2 connections.                                     |
| rsa1      | Displays the RSA algorithm public key for SSH version 1 connections.                                     |

**Mode** User Exec, Privileged Exec and Global Configuration

**Examples** To show the public keys generated on the device for SSH server, use the command:

```
awplus# show crypto key hostkey
```

To display the RSA public key of the SSH server, use the command:

```
awplus# show crypto key hostkey rsa
```

**Output** Figure 25-1: Example output from the **show crypto key hostkey** command

| Type | Bits | Fingerprint                                     |
|------|------|---|
| rsa  | 2058 | 4e:7d:1d:00:75:79:c5:cb:c8:58:2e:f9:29:9c:1f:48 |
| dsa  | 1024 | fa:72:3d:78:35:14:cb:9a:1d:ca:1c:83:2c:7d:08:43 |
| rsa1 | 1024 | e2:1c:c8:8b:d8:6e:19:c8:f4:ec:00:a2:71:4e:85:8b |

**Table 1:** Parameters in output of the **show crypto key hostkey** command

| Parameter   | Description                         |
|-------------|-------------------------------------|
| Type        | Algorithm used to generate the key. |
| Bits        | Length in bits of the key.          |
| Fingerprint | Checksum value for the public key.  |

**Related commands** [crypto key destroy hostkey](#)  
[crypto key generate hostkey](#)

# show crypto key pubkey-chain userkey

**Overview** This command displays the public keys registered with the SSH server for SSH users. These keys allow remote users to access the device using public key authentication. By using public key authentication, users can access the SSH server without providing password.

**Syntax** `show crypto key pubkey-chain userkey <username> [<1-65535>]`

| Parameter  | Description  |
|------------|--|
| <username> | User name of the remote SSH user whose keys you wish to display. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. |
| <1-65535>  | Key identifier for a specific key.   |

**Default** Display all keys.

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the public keys for the user `manager` that are registered with the SSH server, use the command:

```
awplus# show crypto key pubkey-chain userkey manager
```

**Output** Figure 25-2: Example output from the **show crypto key public-chain userkey** command

| No | Type | Bits | Fingerprint                                     |
|----|------|------|---|
| 1  | dsa  | 1024 | 2b:cc:df:a8:f8:2e:8f:a4:a5:4f:32:ea:67:29:78:fd |
| 2  | rsa  | 2048 | 6a:ba:22:84:c1:26:42:57:2c:d7:85:c8:06:32:49:0e |

**Table 2:** Parameters in the output of the **show crypto key userkey** command

| Parameter   | Description                             |
|-------------|---|
| No          | Number ID of the key.                   |
| Type        | The algorithm used to generate the key. |
| Bits        | Length in bits of the key.              |
| Fingerprint | Checksum value for the key.             |

**Related commands** [crypto key pubkey-chain userkey](#)



# show crypto key userkey

**Overview** This command displays the public keys created on this device for the specified SSH user.

**Syntax** `show crypto key userkey <username> [dsa|rsa|rsa1]`

| Parameter  | Description   |
|------------|---|
| <username> | User name of the local SSH user whose keys you wish to display. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. |
| dsa        | Displays the DSA public key.  |
| rsa        | Displays the RSA public key used for SSH version 2 connections.   |
| rsa1       | Displays the RSA key used for SSH version 1 connections.  |

**Mode** User Exec, Privileged Exec and Global Configuration

**Examples** To show the public key generated for the user, use the command:

```
awplus# show crypto key userkey manager
```

To store the RSA public key generated for the user manager to the file "user.pub", use the command:

```
awplus# show crypto key userkey manager rsa > manager-rsa.pub
```

**Output** Figure 25-3: Example output from the **show crypto key userkey** command

| Type | Bits | Fingerprint                                     |
|------|------|---|
| rsa  | 2048 | e8:d6:1b:c0:f4:b6:e6:7d:02:2e:a9:d4:a1:ca:3b:11 |
| rsa1 | 1024 | 12:25:60:95:64:08:8e:a1:8c:3c:45:1b:44:b9:33:9b |

**Table 3:** Parameters in the output of the **show crypto key userkey** command

| Parameter   | Description                             |
|-------------|---|
| Type        | The algorithm used to generate the key. |
| Bits        | Length in bits of the key.              |
| Fingerprint | Checksum value for the key.             |

**Related commands** [crypto key generate userkey](#)

# show running-config ssh

**Overview** This command displays the current running configuration of Secure Shell (SSH).

**Syntax** show running-config ssh

**Mode** Privileged Exec and Global Configuration

**Example** To display the current configuration of SSH, use the command:

```
awplus# show running-config ssh
```

**Output** Figure 25-4: 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 4:** Parameters in the output of the **show running-config ssh** command

| Parameter                              | Description   |
|--|---|
| ssh server                             | SSH server is enabled.  |
| ssh server v2                          | SSH server is enabled and only support SSHv2.                               |
| ssh server<port>                       | SSH server is enabled and listening on the specified TCP port.              |
| no ssh server scp                      | SCP service is disabled.  |
| no ssh server sftp                     | SFTP service is disabled.   |
| ssh server session-timeout             | Configure the server session timeout.                                       |
| ssh server login-timeout               | Configure the server login timeout.   |
| ssh server max-startups                | Configure the maximum number of concurrent sessions waiting authentication. |
| no ssh server authentication password  | Password authentication is disabled.  |
| no ssh server authentication publickey | Public key authentication is disabled.                                      |

**Table 4:** Parameters in the output of the **show running-config ssh** command

| Parameter              | Description                                    |
|------------------------|--|
| ssh server allow-users | Add the user (and hostname) to the allow list. |
| ssh server deny-users  | Add the user (and hostname) to the deny list.  |

**Related commands**

- service ssh
- show ssh server

# show ssh

**Overview** This command displays the active SSH sessions on the device, both incoming and outgoing.

**Syntax** `show ssh`

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the current SSH sessions on the device, use the command:

```
awplus# show ssh
```

**Output** Figure 25-5: Example output from the **show ssh** command

| Secure Shell Sessions: |      |        |              |          |          |             |  |
|------------------------|------|--------|--------------|----------|----------|-------------|--|
| ID                     | Type | Mode   | Peer Host    | Username | State    | Filename    |  |
| 414                    | ssh  | server | 172.16.23.1  | root     | open     |             |  |
| 459                    | scp  | client | 172.16.23.12 | root     | download | example.awd |  |

**Table 5:** Parameters in the output of the **show ssh** command

| Parameter | Description  |
|-----------|--|
| ID        | Unique identifier for each SSH session.  |
| Type      | Session type; either SSH, SCP, or SFTP.  |
| Mode      | Whether the device is acting as an SSH client (client) or SSH server (server) for the specified session. |
| Peer Host | The hostname or IP address of the remote server or client.   |
| Username  | Login user name of the server.   |

**Table 5:** Parameters in the output of the **show ssh** command (cont.)

| Parameter | Description   |   |
|-----------|---|---|
| State     | The current state of the SSH session. One of:                         |   |
|           | connecting  | The device is looking for a remote server.      |
|           | connected   | The device is connected to the remote server.   |
|           | accepted  | The device has accepted a new session.          |
|           | host-auth   | host-to-host authentication is in progress.     |
|           | user-auth   | User authentication is in progress.             |
|           | authenticated   | User authentication is complete.                |
|           | open  | The session is in progress.                     |
|           | download  | The user is downloading a file from the device. |
|           | upload  | The user is uploading a file from the device.   |
|           | closing   | The user is terminating the session.            |
|           | closed  | The session is closed.                          |
| Filename  | Local filename of the file that the user is downloading or uploading. |   |

**Related commands** [clear ssh](#)

# show ssh 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 25-6: Example output from the **show ssh server** command

```
Secure Shell Server Configuration
-----
SSH Server           : Enabled
Port                 : 22
Version              : 2
Services              : scp, sftp
User Authentication  : publickey, password
Resolve Hosts        : Disabled
Session Timeout      : 0 (Off)
Login Timeout        : 60 seconds
Maximum Authentication Tries : 6
Maximum Startups     : 10
Debug                : NONE
```

**Table 6:** Parameters in the output of the **show ssh server** command

| Parameter      | Description  |
|----------------|--|
| SSH Server     | Whether the Secure Shell server is enabled or disabled.  |
| Port           | TCP port where the Secure Shell server listens for connections. The default is port 22.  |
| Version        | SSH server version; either "1", "2" or "2,1".  |
| Services       | List of the available Secure Shell service; one or more of SHELL, SCP or SFTP.   |
| Authentication | List of available authentication methods.  |
| Login Timeout  | Time (in seconds) that the SSH server will wait the SSH session to establish. If the value is 0, the client login will be terminated when TCP timeout reaches. |

**Table 6:** Parameters in the output of the **show ssh server** command (cont.)

| Parameter        | Description  |
|------------------|--|
| Idle Timeout     | Time (in seconds) that the SSH server will wait to receive data from the SSH client. The server disconnects if this timer limit is reached. If set at 0, the idle timer remains off. |
| Maximum Startups | The maximum number of concurrent connections that are waiting authentication. The default is 10.   |
| Debug            | Whether debugging is active on the server.   |

**Related commands** [show ssh](#)

# 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 25-7: Example output from the **show ssh server allow-users** command

| Username | Remote Hostname (pattern) |
|----------|---------------------------|
| awplus   | 192.168.*                 |
| john     |                           |
| manager  | *.alliedtelesis.com       |

**Table 7:** Parameters in the output of the **show ssh server allow-users** command

| Parameter                 | Description   |
|---------------------------|---|
| Username                  | User name that is allowed to access the SSH server.   |
| Remote Hostname (pattern) | IP address or hostname pattern of the remote client. The user is allowed requests from a host that matches this pattern. If no hostname is specified, the user is allowed from all hosts. |

**Related commands** [ssh server allow-users](#)  
[ssh server deny-users](#)



# show ssh server deny-users

**Overview** This command displays the user entries in the deny list of the SSH server. The user in the deny list is rejected to access the SSH server. If a user is not included in the access list of the SSH server, the user is also rejected.

**Syntax** `show ssh server deny-users`

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the user entries in the deny list of the SSH server, use the command:

```
awplus# show ssh server deny-users
```

**Output** Figure 25-8: Example output from the **show ssh server deny-users** command

| Username | Remote Hostname (pattern) |
|----------|---------------------------|
| john     | *.b-company.com           |
| manager  | 192.168.2.*               |

**Table 8:** Parameters in the output of the **show ssh server deny-user** command

| Parameter                 | Description   |
|---------------------------|---|
| Username                  | The user that this rule applies to.   |
| Remote Hostname (pattern) | IP address or hostname pattern of the remote client. The user is denied requests from a host that matches this pattern. If no hostname is specified, the user is denied from all hosts. |

**Related commands** [ssh server allow-users](#)  
[ssh server deny-users](#)

# ssh server

**Overview** Use this command to modify the configuration of the SSH server. Changing these parameters affects new SSH sessions connecting to the device.

Use the **no** variant of this command to restore the configuration of a specified parameter to its default. The change affects the SSH server immediately if the server is running. Otherwise, the configuration is used when the server starts.

To enable the SSH server, use the [service ssh](#) command.

**Syntax**

```
ssh server {[v1v2|v2only]|<1-65535>}
ssh server {[session-timeout <0-3600>] [login-timeout <1-600>]
[max-startups <1-128>]}
no ssh server {[session-timeout] [login-timeout]
[max-startups]}
```

| Parameter       | Description   |
|-----------------|---|
| v1v2            | Supports both SSHv2 and SSHv1 client connections.<br>Default: v1v2  |
| v2only          | Supports SSHv2 client connections only.   |
| <1-65535>       | The TCP port number that the server listens to for incoming SSH sessions.<br>Default: 22  |
| session-timeout | The maximum time period that the server waits before deciding that a session is inactive and should be terminated. The server considers the session inactive when it has not received any data from the client, and when the client does not respond to keep alive messages.<br>Default: 0 (session timer remains off). |
|                 | <0-3600> Timeout in seconds.  |
| login-timeout   | The maximum time period the server waits before disconnecting an unauthenticated client.<br>Default: 60   |
|                 | <1-600> Timeout in seconds.   |
| max-startups    | The maximum number of concurrent unauthenticated connections the server accepts. When the number of SSH connections awaiting authentication reaches the limit, the server drops any additional connections until authentication succeeds or the login timer expires for a connection.<br>Default: 10                    |
|                 | <1-128> Number of sessions.   |

**Mode** Global Configuration

**Examples** To configure the session timer of SSH server to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 600
```

To configure the login timeout of SSH server to 30 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 30
```

To limit the number of SSH client connections waiting for authentication from SSH server to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-startups 3
```

To set max-startups parameters of SSH server to the default configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server max-startups
```

To support the Secure Shell server with TCP port 2200, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server 2200
```

To force the Secure Shell server to support SSHv2 only, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server v2only
```

To support both SSHv2 and SSHv1, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server v1v2
```

**Related commands** [show ssh server](#)

# ssh server allow-users

**Overview** This command adds a username pattern to the allow list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is accepted.

When there are no registered users in the server's database of allowed users, the SSH server does not accept SSH sessions even when enabled.

SSH server also maintains the deny list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

The **no** variant of this command deletes a username pattern from the allow list of the SSH server. To delete an entry from the allow list, the username and hostname pattern should match exactly with the existing entry.

**Syntax** `ssh server allow-users <username-pattern> [<hostname-pattern>]`  
`no ssh server allow-users <username-pattern>`  
`[<hostname-pattern>]`

| Parameter                             | Description  |
|---------------------------------------|--|
| <code>&lt;username-pattern&gt;</code> | The username pattern that users can match to. An asterisk acts as a wildcard character that matches any string of characters.  |
| <code>&lt;hostname-pattern&gt;</code> | The host name pattern that hosts can match to. If specified, the server allows the user to connect only from hosts matching the pattern. An asterisk acts as a wildcard character that matches any string of characters. |

**Mode** Global Configuration

**Examples** To allow the user `john` to create an SSH session from any host, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john
```

To allow the user `john` to create an SSH session from a range of IP address (from 192.168.1.1 to 192.168.1.255), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john 192.168.1.*
```

To allow the user `john` to create a SSH session from a `a-company.com` domain, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john *.a-company.com
```

To delete the existing user entry `john 192.168.1.*` in the allow list, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no ssh server allow-users john 192.168.1.*
```

**Related  
commands**

[show running-config ssh](#)

[show ssh server allow-users](#)

[ssh server deny-users](#)

# ssh server authentication

**Overview** This command enables RSA public-key or password user authentication for SSH Server. Apply the **password** keyword with the **ssh server authentication** command to enable password authentication for users. Apply the **publickey** keyword with the **ssh server authentication** command to enable RSA public-key authentication for users.

Use the **no** variant of this command to disable RSA public-key or password user authentication for SSH Server. Apply the **password** keyword with the **no ssh authentication** command to disable password authentication for users. Apply the required **publickey** keyword with the **no ssh authentication** command to disable RSA public-key authentication for users.

**Syntax** `ssh server authentication {password|publickey}`  
`no ssh server authentication {password|publickey}`

| Parameter | Description   |
|-----------|---|
| password  | Specifies user password authentication for SSH server.  |
| publickey | Specifies user publickey authentication for SSH server. |

**Default** Both RSA public-key authentication and password authentication are enabled by default.

**Mode** Global Configuration

**Usage** For password authentication to authenticate a user, password authentication for a user must be registered in the local user database or on an external RADIUS server, before using the **ssh server authentication password** command.

For RSA public-key authentication to authenticate a user, a public key must be added for the user, before using the **ssh server authentication publickey** command.

**Examples** To enable `password` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server authentication password
```

To enable `publickey` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server authentication publickey
```

To disable password authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server authentication password
```

To disable publickey authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server authentication publickey
```

**Related  
commands**

[crypto key pubkey-chain userkey](#)  
[service ssh](#)  
[show ssh server](#)

# ssh server deny-users

**Overview** This command adds a username pattern to the deny list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is rejected.

SSH server also maintains the allow list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

If a hostname pattern is specified, the user is denied from the hosts matching the pattern.

The **no** variant of this command deletes a username pattern from the deny list of the SSH server. To delete an entry from the deny list, the username and hostname pattern should match exactly with the existing entry.

**Syntax** `ssh server deny-users <username-pattern> [<hostname-pattern>]`  
`no ssh server deny-users <username-pattern>`  
`[<hostname-pattern>]`

| Parameter                             | Description   |
|---------------------------------------|---|
| <code>&lt;username-pattern&gt;</code> | The username pattern that users can match to. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen, full stop and asterisk symbols. An asterisk acts as a wildcard character that matches any string of characters. |
| <code>&lt;hostname-pattern&gt;</code> | The host name pattern that hosts can match to. If specified, the server denies the user only when they connect from hosts matching the pattern. An asterisk acts as a wildcard character that matches any string of characters.   |

**Mode** Global Configuration

**Examples** To deny the user john to access SSH login from any host, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john
```

To deny the user john to access SSH login from a range of IP address (from 192.168.2.1 to 192.168.2.255), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john 192.168.2.*
```

To deny the user john to access SSH login from b-company.com domain, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john*.b-company.com
```



To delete the existing user entry `john 192.168.2.*` in the deny list, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no ssh server deny-users john 192.168.2.*
```

**Related commands**

- [show running-config ssh](#)
- [show ssh server deny-users](#)
- [ssh server allow-users](#)

# ssh server max-auth-tries

**Overview** Use this command to specify the maximum number of SSH authentication attempts that the device will allow.

Use the **no** variant of this command to return the maximum number of attempts to its default value of 6.

**Syntax** `ssh server max-auth-tries <1-32>`  
`no ssh server max-auth-tries`

| Parameter | Description  |
|-----------|--|
| <1-32>    | Maximum number of SSH authentication attempts the device will allow. |

**Default** 6 attempts

**Mode** Global Configuration

**Usage** By default, users must wait one second after a failed login attempt before trying again. You can increase this gap by using the command [aaa login fail-delay](#).

**Example** To set the maximum number of SSH authentication attempts to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-auth-tries 3
```

**Related commands** [show ssh server](#)

# ssh server resolve-host

**Overview** This command enables resolving an IP address from a host name using a DNS server for client host authentication.

The **no** variant of this command disables this feature.

**Syntax** `ssh server resolve-hosts`  
`no ssh server resolve-hosts`

**Default** This feature is disabled by default.

**Mode** Global Configuration

**Usage notes** Your device has a DNS Client that is enabled automatically when you add a DNS server to your device. Use the [ip name-server](#) command to add a DNS server to the list of servers that the device queries.

**Example** To resolve a host name using a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server resolve-hosts
```

**Related commands**

- [ip name-server](#)
- [show ssh server](#)
- [ssh server allow-users](#)
- [ssh server deny-users](#)

# ssh server scp

**Overview** This command enables the Secure Copy (SCP) service on the SSH server. Once enabled, the server accepts SCP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SCP connections. The SCP service is enabled by default as soon as the SSH server is enabled.

The **no** variant of this command disables the SCP service on the SSH server. Once disabled, SCP requests from remote clients are rejected.

**Syntax** `ssh server scp`  
`no ssh server scp`

**Mode** Global Configuration

**Examples** To enable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server scp
```

To disable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server scp
```

**Related commands** [show running-config ssh](#)  
[show ssh server](#)

# ssh server sftp

**Overview** This command enables the Secure FTP (SFTP) service on the SSH server. Once enabled, the server accepts SFTP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SFTP connections. The SFTP service is enabled by default as soon as the SSH server is enabled. If the SSH server is disabled, SFTP service is unavailable.

The **no** variant of this command disables SFTP service on the SSH server. Once disabled, SFTP requests from remote clients are rejected.

**Syntax** `ssh server sftp`  
`no ssh server sftp`

**Mode** Global Configuration

**Examples** To enable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server sftp
```

To disable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server sftp
```

**Related commands** [show running-config ssh](#)  
[show ssh server](#)

# undebug ssh server

**Overview** This command applies the functionality of the **no debug ssh server** command.

# 26

# Trigger Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure Triggers. For more information, see the [Triggers Feature Overview and Configuration Guide](#).

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

- Command List**
- [“active \(trigger\)”](#) on page 1153
  - [“day”](#) on page 1154
  - [“debug trigger”](#) on page 1156
  - [“description \(trigger\)”](#) on page 1157
  - [“repeat”](#) on page 1158
  - [“script”](#) on page 1159
  - [“show debugging trigger”](#) on page 1161
  - [“show running-config trigger”](#) on page 1162
  - [“show trigger”](#) on page 1163
  - [“test”](#) on page 1168
  - [“time \(trigger\)”](#) on page 1169
  - [“trap”](#) on page 1171
  - [“trigger”](#) on page 1172
  - [“trigger activate”](#) on page 1173
  - [“type atmf node”](#) on page 1174
  - [“type cpu”](#) on page 1177
  - [“type interface”](#) on page 1178
  - [“type linkmon-probe”](#) on page 1179

- [“type log”](#) on page 1181
- [“type memory”](#) on page 1182
- [“type periodic”](#) on page 1183
- [“type ping-poll”](#) on page 1184
- [“type reboot”](#) on page 1185
- [“type time”](#) on page 1186
- [“type usb”](#) on page 1187
- [“undebg trigger”](#) on page 1188



# active (trigger)

**Overview** This command enables a trigger. This allows the trigger to activate when its trigger conditions are met.

The **no** variant of this command disables a trigger. While in this state the trigger cannot activate when its trigger conditions are met.

**Syntax** active  
no active

**Default** Active, which means that triggers are enabled by default

**Mode** Trigger Configuration

**Usage notes** Configure a trigger first before you use this command to activate it.

For information about configuring a trigger, see the [Triggers\\_Feature Overview and Configuration Guide](#).

**Examples** To enable trigger 172, so that it can activate when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 172
awplus(config-trigger)# active
```

To disable trigger 182, preventing it from activating when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 182
awplus(config-trigger)# no active
```

**Related commands** [show trigger](#)  
[trigger](#)  
[trigger activate](#)

# day

**Overview** This command specifies the days or date that the trigger can activate on. You can specify one of:

- A specific date
- A specific day of the week
- A list of days of the week
- A day of any month of any year
- A day of a specific month in any year
- Every day

By default, the trigger can activate on any day.

**Syntax** `day every-day`  
`day <1-31>`  
`day <1-31> <month>`  
`day <1-31> <month> <year>`  
`day <weekday>`

| Parameter                    | Description   |
|------------------------------|---|
| <code>every-day</code>       | Sets the trigger so that it can activate on any day.  |
| <code>&lt;1-31&gt;</code>    | Day of the month the trigger is permitted to activate on.   |
| <code>&lt;month&gt;</code>   | Sets the month that the trigger is permitted to activate on. Valid keywords are: <b>january, february, march, april, may, june, july, august, september, october, november, and december.</b>                               |
| <code>&lt;year&gt;</code>    | Sets the year that the trigger is permitted to activate in, between 2000 and 2035.  |
| <code>&lt;weekday&gt;</code> | Sets the days of the week that the trigger can activate on. You can specify one or more week days in a space separated list. Valid keywords are: <b>monday, tuesday, wednesday, thursday, friday, saturday, and sunday.</b> |

**Default** **every-day**, so by default, the trigger can activate on any day.

**Mode** Trigger Configuration

**Usage notes** For example trigger configurations that use the **day** command, see “Restrict Internet Access” and “Turn off Power to Port LEDs” in the [Triggers Feature Overview and Configuration Guide](#).

**Examples** To permit trigger 55 to activate on the 1 June 2019, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 55
awplus(config-trigger)# day 1 jun 2019
```

To permit trigger 12 to activate on Mondays, Wednesdays and Fridays, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# day monday wednesday friday
```

To permit trigger 17 to activate on the 5th day of any month, in any year, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 17
awplus(config-trigger)# day 5
```

To permit trigger 6 to activate on the 20th day of September, in any year, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 6
awplus(config-trigger)# day 20 september
```

To permit trigger 14 to activate on the 1st day of each month, in any year, at 11.00am, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 14
awplus(config-trigger)# day 1
awplus(config-trigger)# type time 11:00
```

**Related commands** [show trigger](#)  
[type time](#)  
[trigger](#)

**Command changes** Version 5.4.8-2.1: day of the month functionality added

# debug trigger

**Overview** This command enables trigger debugging. This generates detailed messages about how your device is processing the trigger commands and activating the triggers.

The **no** variant of this command disables trigger debugging.

**Syntax** debug trigger  
no debug trigger

**Mode** Privilege Exec

**Examples** To start trigger debugging, use the command:

```
awplus# debug trigger
```

To stop trigger debugging, use the command:

```
awplus# no trigger
```

**Related commands** [show debugging trigger](#)  
[show trigger](#)  
[test](#)  
[trigger](#)  
[undebug trigger](#)

# description (trigger)

**Overview** This command adds an optional description to help you identify the trigger. This description is displayed in show command outputs and log messages.

The **no** variant of this command removes a trigger's description. The show command outputs and log messages stop displaying a description for this trigger.

**Syntax** `description <description>`  
`no description`

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;description&gt;</code> | A word or phrase that uniquely identifies this trigger or its purpose. Valid characters are any printable character and spaces, up to a maximum of 40 characters. |

**Mode** Trigger Configuration

**Examples** To give trigger 240 the description `daily status report`, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 240
awplus(config-trigger)# description daily status report
```

To remove the description from trigger 36, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 36
awplus(config-trigger)# no description
```

**Related commands** [show trigger](#)  
[test](#)  
[trigger](#)

# repeat

**Overview** This command specifies the number of times that a trigger is permitted to activate. This allows you to specify whether you want the trigger to activate:

- only the first time that the trigger conditions are met
- a limited number of times that the trigger conditions are met
- an unlimited number of times

Once the trigger has reached the limit set with this command, the trigger remains in your configuration but cannot be activated. Use the **repeat** command again to reset the trigger so that it is activated when its trigger conditions are met.

By default, triggers can activate an unlimited number of times. To reset a trigger to this default, specify either **yes** or **forever**.

**Syntax** `repeat { forever | no | once | yes | <1-4294967294> }`

| Parameter      | Description  |
|----------------|--|
| yes   forever  | The trigger repeats indefinitely, or until disabled. |
| no   once      | The trigger activates only once.                     |
| <1-4292967294> | The trigger repeats the specified number of times.   |

**Mode** Trigger Configuration

**Examples** To allow trigger 21 to activate only once, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 21
awplus(config-trigger)# repeat no
```

To allow trigger 22 to activate an unlimited number of times whenever its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 22
awplus(config-trigger)# repeat forever
```

To allow trigger 23 to activate only the first 10 times the conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 23
awplus(config-trigger)# repeat 10
```

**Related commands** [show trigger](#)  
[trigger](#)

# script

**Overview** This command specifies one or more scripts that are to be run when the trigger activates. You can add up to five scripts to a single trigger.

The sequence in which the trigger runs the scripts is specified by the number you set before the name of the script file. One script is executed completely before the next script begins.

Scripts may be either ASH shell scripts, indicated by a **.sh** filename extension suffix, or AlliedWare Plus™ scripts, indicated by a **.scp** filename extension suffix. AlliedWare Plus™ scripts only need to be readable.

The **no** variant of this command removes one or more scripts from the trigger's script list. The scripts are identified by either their name, or by specifying their position in the script list. The **all** parameter removes all scripts from the trigger.

**Syntax** `script <1-5> {<filename>}`  
`no script {<1-5>|<filename>|all}`

| Parameter  | Description  |
|------------|--|
| <1-5>      | The position of the script in execution sequence. The trigger runs the lowest numbered script first. |
| <filename> | The path to the script file.   |

**Mode** Trigger Configuration

**Examples** To configure trigger 71 to run the script `flash:/cpu_trig.sh` in position 3 when the trigger activates, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# script 3 flash:/cpu_trig.sh
```

To configure trigger 99 to run the scripts **flash:reconfig.scp**, **flash:cpu\_trig.sh** and **flash:email.scp** in positions 2, 3 and 5 when the trigger activates, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 99
awplus(config-trigger)# script 2 flash:/reconfig.scp 3
flash:/cpu_trig.sh 5 flash:/email.scp
```

To remove the scripts 1, 3 and 4 from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script 1 3 4
```

To remove the script flash:/cpu\_trig.sh from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script flash:/cpu_trig.sh
```

To remove all the scripts from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script all
```

**Related commands** [show trigger](#)  
[trigger](#)



# show debugging trigger

**Overview** This command displays the current status for trigger utility debugging. Use this command to show when trigger debugging has been turned on or off from the [debug trigger](#) command.

**Syntax** show debugging trigger

**Mode** User Exec and Privileged Exec

**Example** To display the current configuration of trigger debugging, use the command:

```
awplus# show debugging trigger
```

**Output** Figure 26-1: Example output from the **show debugging trigger** command

```
awplus#debug trigger
awplus#show debugging trigger
Trigger debugging status:
  Trigger debugging is on

awplus#no debug trigger
awplus#show debugging trigger
Trigger debugging status:
  Trigger debugging is off
```

**Related commands** [debug trigger](#)

# show running-config trigger

**Overview** This command displays the current running configuration of the trigger utility.

**Syntax** show running-config trigger

**Mode** Privileged Exec

**Example** To display the current configuration of the trigger utility, use the command:

```
awplus# show running-config trigger
```

Figure 26-2: Example output from the **show running-config trigger** command

```
trigger 1
  type card in

type usb in
trigger 2

type usb out
!
```

**Related commands** [show trigger](#)

# show trigger

**Overview** This command displays configuration and diagnostic information about the triggers configured on the device. Specify the **show trigger** command without any options to display a summary of the configuration of all triggers.

**Syntax** `show trigger [<1-250>|counter|full]`

| Parameter | Description   |
|-----------|---|
| <1-250>   | Displays detailed information about a specific trigger, identified by its trigger ID. |
| counter   | Displays statistical information about all triggers.                                  |
| full      | Displays detailed information about all triggers.                                     |

**Mode** Privileged Exec

**Example** To get summary information about all triggers, use the following command:

```
awplus# show trigger
```

Table 26-1: Example output from **show trigger**

```
awplus#show trigger
TR# Type & Details      Name                Ac Te Repeat      #Scr Days/Date
-----
001 CPU (80% any)       Busy CPU            Y  N  5              1 smtwtfS
005 Periodic (30 min)   Regular status check Y  N  Continuous     1 -mtwtf-
007 Memory (85% up)     High mem usage      Y  N  8              1 smtwtfS
011 Time (00:01)        Weekend access      Y  N  Continuous     1 -----s
013 Reboot              Y  N  Continuous     2 smtwtfS
017 Interface (vlan1 .. Change config for... Y  N  Once           1 2-apr-2008
019 Ping-poll (5 up)    Connection to svr1  Y  N  Continuous     1 smtwtfS
-----
```

Table 26-2: Parameters in the output of **show trigger**

| Parameter      | Description  |
|----------------|--|
| TR#            | Trigger identifier (ID).   |
| Type & Details | The trigger type, followed by the trigger details in brackets.                                     |
| Name           | Descriptive name of the trigger configured with the <a href="#">description (trigger)</a> command. |
| Ac             | Whether the trigger is active (Y), or inactive (N).  |

Table 26-2: Parameters in the output of **show trigger** (cont.)

| Parameter | Description   |
|-----------|---|
| Te        | Whether the trigger is in test mode (Y) or not (N).   |
| Repeat    | Whether the trigger repeats continuously, and if not, the configured repeat count for the trigger. To see the number of times a trigger has activated, use the <b>show trigger</b> <1-250> command.                 |
| #Scr      | Number of scripts associated with the trigger.  |
| Days/Date | Days or date when the trigger may be activated. For the days options, the days are shown as a seven character string representing Sunday to Saturday. A hyphen indicates days when the trigger cannot be activated. |

To display detailed information about trigger 3, use the command:

```
awplus# show trigger 3
```

Figure 26-3: Example output from **show trigger** for a specific trigger

```
awplus#show trigger 1
Trigger Configuration Details
-----
Trigger ..... 1
Name ..... display cpu usage when pass 80%
Type and details ..... CPU (80% up)
Days ..... smtwfss
Active ..... Yes
Test ..... No
Trap ..... Yes
Repeat ..... Continuous
Modified ..... Fri Feb 3 17:18:44 2017
Number of activations ..... 0
Last activation ..... not activated
Number of scripts ..... 1
1. shocpu.scp
2.
3.
4.
5.
-----
```

To display detailed information about all triggers, use the command:

```
awplus# show trigger full
```

Table 26-3: Example output from **show trigger full**

```
awplus#show trigger full
Trigger Configuration Details
-----
Trigger ..... 1
Name ..... Busy CPU
Type and details ..... CPU (80% up)
Days ..... smtwtfS
Active ..... Yes
Test ..... No
Trap ..... Yes
Repeat ..... Continuous
Modified ..... Fri Feb 3 17:05:16 2017
Number of activations ..... 0
Last activation ..... not activated
Number of scripts ..... 2
  1. flash:/cpu_alert.sh
  2. flash:/reconfig.scp
  3.
  4.
  5.
Trigger ..... 5
Name ..... Regular status check
Type and details ..... Periodic (30 min)
Days ..... smtwtfS
Active ..... Yes
Test ..... No
Trap ..... Yes
Repeat ..... 5 (2)
Modified ..... Fri Feb 3 17:18:44 2017
Number of activations ..... 0
Last activation ..... Fri Feb 10 18:00:00 2017
Number of scripts ..... 1
  1. flash:/stat_check.scp
  2.
  3.
  4.
  5.
-----
```

Table 27: Parameters in the output of **show trigger full** and **show trigger** for a specific trigger

| Parameter        | Description   |
|------------------|---|
| Trigger          | The ID of the trigger.                                  |
| Name             | Descriptive name of the trigger.                        |
| Type and details | The trigger type and its activation conditions.         |
| Days             | The days on which the trigger is permitted to activate. |

**Table 27:** Parameters in the output of **show trigger full** and **show trigger** for a specific trigger (cont.)

| Parameter             | Description   |
|-----------------------|---|
| Date                  | The date on which the trigger is permitted to activate. Only displayed if configured, in which case it replaces "Days".   |
| Active                | Whether or not the trigger is permitted to activate.  |
| Test                  | Whether or not the trigger is operating in diagnostic mode.   |
| Trap                  | Whether or not the trigger is enabled to send SNMP traps.   |
| Repeat                | Whether the trigger repeats an unlimited number of times (Continuous) or for a set number of times. When the trigger can repeat only a set number of times, then the number of times the trigger has been activated is displayed in brackets. |
| Modified              | The date and time of the last time that the trigger was modified.   |
| Number of activations | Number of times the trigger has been activated since the last restart of the device.  |
| Last activation       | The date and time of the last time that the trigger was activated.  |
| Number of scripts     | How many scripts are associated with the trigger, followed by the names of the script files in the order in which they run.   |

To display counter information about all triggers use the command:

```
awplus# show trigger counter
```

**Figure 26-4:** Example output from **show trigger counter**

```
awplus# show trigger counter
Trigger Module Counters
-----
Trigger activations                4
Last trigger activated            55
Time triggers activated today     0
Periodic triggers activated today 0
Interface triggers activated today 1
CPU triggers activated today      2
Memory triggers activated today   1
Reboot triggers activated today   0
Ping-poll triggers activated today 0
USB event triggers activated today 0
Stack master fail triggers activated today 0
Stack member triggers activated today 0
Stack link triggers activated today 0
ATMF node triggers activated today 0
Log triggers activated today      0
-----
```

**Related  
commands** [active \(trigger\)](#)  
[debug trigger](#)  
[script](#)  
[trigger](#)  
[trigger activate](#)

# test

**Overview** This command puts the trigger into a diagnostic mode. In this mode the trigger may activate but when it does it will not run any of the trigger's scripts. A log message will be generated to indicate when the trigger has been activated.

The **no** variant of this command takes the trigger out of diagnostic mode, restoring normal operation. When the trigger activates the scripts associated with the trigger will be run, as normal.

**Syntax** test  
no test

**Mode** Trigger Configuration

**Usage notes** Configure a trigger first before you use this command to diagnose it. For information about configuring a trigger, see the [Triggers\\_Feature Overview and Configuration Guide](#).

**Examples** To put trigger 5 into diagnostic mode, where no scripts will be run when the trigger activates, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# test
```

To take trigger 205 out of diagnostic mode, restoring normal operation, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no test
```

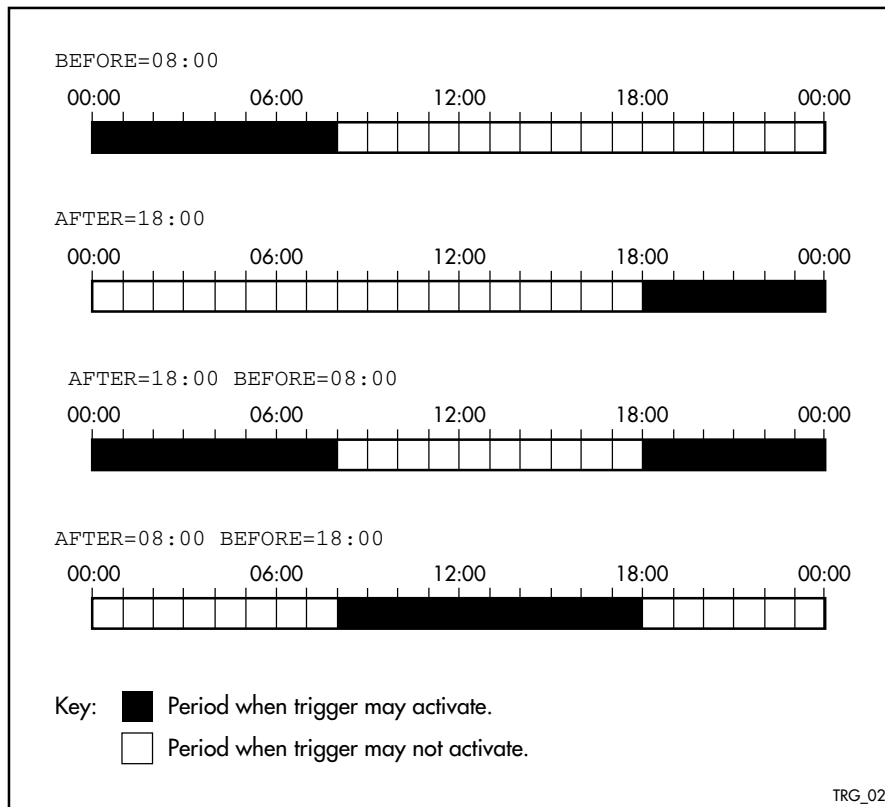
**Related commands** [show trigger](#)  
[trigger](#)



# time (trigger)

**Overview** This command specifies the time of day when the trigger is permitted to activate. The **after** parameter specifies the start of a time period that extends to midnight during which trigger may activate. By default the value of this parameter is 00:00:00 (am); that is, the trigger may activate at any time. The **before** parameter specifies the end of a time period beginning at midnight during which the trigger may activate. By default the value of this parameter is 23:59:59; that is, the trigger may activate at any time. If the value specified for **before** is later than the value specified for **after**, a time period from “after” to “before” is defined, during which the trigger may activate. This command is not applicable to time triggers (**type time**).

The following figure illustrates how the **before** and **after** parameters operate.



**Syntax** `time { [after <hh:mm:ss> ] [before <hh:mm:ss> ] }`

| Parameter                           | Description   |
|-------------------------------------|---|
| <code>after&lt;hh:mm:ss&gt;</code>  | The earliest time of day when the trigger may be activated. |
| <code>before&lt;hh:mm:ss&gt;</code> | The latest time of day when the trigger may be activated.   |

**Mode** Trigger Configuration

**Usage notes** For example trigger configurations that use the **time (trigger)** command, see “Restrict Internet Access” and “Turn off Power to Port LEDs” in the [Triggers Feature Overview and Configuration Guide](#).

**Examples** To allow trigger 63 to activate between midnight and 10:30am, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 63
awplus(config-trigger)# time before 10:30:00
```

To allow trigger 64 to activate between 3:45pm and midnight, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 64
awplus(config-trigger)# time after 15:45:00
```

To allow trigger 65 to activate between 10:30am and 8:15pm, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 65
awplus(config-trigger)# time after 10:30:00 before 20:15:00
```

**Related commands** [show trigger](#)  
[trigger](#)

# trap

**Overview** This command enables the specified trigger to send SNMP traps.

Use the **no** variant of this command to disable the sending of SNMP traps from the specified trigger.

**Syntax** trap  
no trap

**Default** SNMP traps are enabled by default for all defined triggers.

**Mode** Trigger Configuration

**Usage notes** You must configure SNMP before using traps with triggers. For more information, see:

- [Support for Allied Telesis Enterprise\\_MIBs\\_in\\_AlliedWare Plus](#), for information about which MIB objects are supported.
- the [SNMP Feature Overview and Configuration\\_Guide](#).
- the [SNMP Commands](#) chapter.

Since SNMP traps are enabled by default for all defined triggers, a common usage will be for the **no** variant of this command to disable SNMP traps from a specified trap if the trap is only periodic. Refer in particular to AT-TRIGGER-MIB in the [Support for Allied Telesis Enterprise\\_MIBs\\_in AlliedWare Plus](#) for further information about the relevant SNMP MIB.

**Examples** To enable SNMP traps to be sent from trigger 5, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# trap
```

To disable SNMP traps being sent from trigger 205, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no trap
```

**Related commands** trigger  
show trigger

# trigger

**Overview** This command is used to access the Trigger Configuration mode for the specified trigger. Once Trigger Configuration mode has been entered the trigger type information can be configured and the trigger scripts and other operational parameters can be specified. At a minimum the trigger type information must be specified before the trigger can become active.

The **no** variant of this command removes a specified trigger and all configuration associated with it.

**Syntax** trigger <1-250>  
no trigger <1-250>

| Parameter | Description   |
|-----------|---------------|
| <1-250>   | A trigger ID. |

**Mode** Global Configuration

**Examples** To enter trigger configuration mode for trigger 12, use the commands:

```
awplus# configure terminal  
awplus(config)# trigger 12
```

To completely remove all configuration associated with trigger 12, use the commands:

```
awplus# configure terminal  
awplus(config)# no trigger 12
```

**Related commands** [show trigger](#)  
[trigger activate](#)

# trigger activate

**Overview** This command is used to manually activate a specified trigger from the Privileged Exec mode, which has been configured with the **trigger** command from the Global Configuration mode.

**Syntax** `trigger activate <1-250>`

| Parameter | Description   |
|-----------|---------------|
| <1-250>   | A trigger ID. |

**Mode** Privileged Exec

**Usage notes** This command manually activates a trigger without the normal trigger conditions being met.

The trigger is activated even if it has been configured as inactive by using the command **no active**. The scripts associated with the trigger will be executed even if the trigger is in the diagnostic test mode.

Triggers activated manually do not have their repeat counts decremented or their 'last triggered' time updated, and do not result in updates to the '[type] triggers today' counters.

**Example** To manually activate trigger 12 use the command:

```
awplus# trigger activate 12
```

**Related commands**

- [active \(trigger\)](#)
- [show trigger](#)
- [trigger](#)

# type atmf node

**Overview** This command configures a trigger to be activated at an AMF node join event or leave event.

**Syntax** type atmf node {join|leave}

| Parameter | Description           |
|-----------|-----------------------|
| join      | AMF node join event.  |
| leave     | AMF node leave event. |

**Mode** Trigger Configuration

**CAUTION:** *Only configure this trigger on one device because it is a network wide event.*

**Example 1** To configure trigger 5 to activate at an AMF node leave event, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger) type atmf node leave
```

**Example 2** The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
=====
node1, node2, node3:
=====

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp  
AMF-Net[3](config-trigger)# end
```

Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=====  
node1:  
=====
```

| TR# | Type & Details    | Description         | Ac | Te | Tr | Repeat     | #Scr | Days/Date |
|-----|-------------------|---------------------|----|----|----|------------|------|-----------|
| 001 | Periodic (2 min)  | Periodic Status Chk | Y  | N  | Y  | Continuous | 1    | smtwtfs   |
| 005 | ATMF node (leave) | E-mail on ATMF Exit | Y  | N  | Y  | Continuous | 1    | smtwtfs   |

```
-----  
  
=====  
Node2, Node3,  
=====
```

| TR# | Type & Details    | Description         | Ac | Te | Tr | Repeat     | #Scr | Days/Date |
|-----|-------------------|---------------------|----|----|----|------------|------|-----------|
| 005 | ATMF node (leave) | E-mail on ATMF Exit | Y  | N  | Y  | Continuous | 1    | smtwtfs   |

```
-----
```

Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
=====  
Node1:  
=====  
  
trigger 1  
  type periodic 2  
  script 1 atmf.scp  
trigger 5  
  type atmf node leave  
description "E-mail on ATMF Exit"  
  script 1 email_me.scp  
!  
  
=====  
Node2, Node3:  
=====  
  
trigger 5  
  type atmf node leave  
description "E-mail on ATMF Exit"  
  script 1 email_me.scp  
!
```

**Related commands** [show trigger](#)



# type cpu

**Overview** This command configures a trigger to activate based on CPU usage level. Selecting the **up** option causes the trigger to activate when the CPU usage exceeds the specified usage level. Selecting the **down** option causes the trigger to activate when CPU usage drops below the specified usage level. Selecting **any** causes the trigger to activate in both situations. The default is **any**.

**Syntax** `type cpu <1-100> [up|down|any]`

| Parameter | Description  |
|-----------|--|
| <1-100>   | The percentage of CPU usage at which to trigger.                       |
| up        | Activate when CPU usage exceeds the specified level.                   |
| down      | Activate when CPU usage drops below the specified level                |
| any       | Activate when CPU usage passes the specified level in either direction |

**Mode** Trigger Configuration

**Usage notes** For an example trigger configuration that uses the **type cpu** command, see “Capture Unusual CPU and RAM Activity” in the [Triggers Feature Overview and Configuration Guide](#).

**Examples** To configure trigger 28 to be a CPU trigger that activates when CPU usage exceeds 80% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 28
awplus(config-trigger)# type cpu 80 up
```

To configure trigger 5 to be a CPU trigger that activates when CPU usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65

or

awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65 any
```

**Related commands** [show trigger](#)  
[trigger](#)

# type interface

**Overview** This command configures a trigger to activate based on the link status of an interface. The trigger can be activated when the interface becomes operational by using the **up** option, or when the interface closes by using the **down** option. The trigger can also be configured to activate when either one of these events occurs by using the **any** option.

**Syntax** `type interface <interface> [up|down|any]`

| Parameter   | Description   |
|-------------|---|
| <interface> | Interface name. This can be the name of a device port, an eth-management port, or a VLAN. |
| up          | Activate when interface becomes operational.  |
| down        | Activate when the interface closes.   |
| any         | Activate when any interface link status event occurs.                                     |

**Mode** Trigger Configuration

**Example** To configure trigger 19 to be an interface trigger that activates when port1.0.2 becomes operational, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 19
awplus(config-trigger)# type interface port1.0.2 up
```

**Related commands** [show trigger](#)  
[trigger](#)

# type linkmon-probe

**Overview** Use this command to create a trigger that will run a script when a Link Health Monitoring probe reports that a link becomes “good”, “bad”, or “unreachable”.

**Syntax** `type linkmon-probe <probename> <profilename>  
{good|bad|unreachable|any}`

| Parameter     | Description  |
|---------------|--|
| <probename>   | The name of the Link Health Monitoring probe that will be used for executing the trigger.  |
| <profilename> | The name of the Link Health Monitoring performance profile that will be used for determine if the Link Health Monitoring probe is good, bad, or unreachable. |
| good          | If the Link Health Monitoring probe becomes 'good' according to the Link Health Monitoring performance profile then the trigger will be executed.            |
| bad           | If the Link Health Monitoring probe goes 'bad' according to the Link Health Monitoring performance profile then the trigger will be executed.                |
| unreachable   | If the Link Health Monitoring probe becomes 'unreachable' according to the Link Health Monitoring performance profile then the trigger will be executed.     |
| any           | If the Link Health Monitoring probe changes state according to the Link Health Monitoring performance profile then the trigger will be executed.             |

**Mode** Trigger Configuration

**Example** When the Link Health Monitoring probes sent to the “test-probe” destination no longer meet the performance profile “test-profile” the link will be deemed “bad”. To create a trigger that will run a script when a Link Health Monitoring probe is deemed “bad”, use the following commands:

```
awplus# trigger 1  
awplus(config)# script 1 link-bad.scp  
awplus(config)# type linkmon-probe test-probe test-profile bad
```

To create a trigger that will run a script when the link is deemed “good” again, use the following commands:

```
awplus# trigger 2  
awplus(config)# script 1 link-good.scp  
awplus(config)# type linkmon-probe test-probe test-profile good
```

**Related commands** [trigger](#)

**Command changes** Version 5.4.8-1.1: command added

# type log

**Overview** Use this command to configure a trigger to activate based on the content of log messages matching a string or regular expression.

**Syntax** `type log <log-message-string>`

| Parameter                               | Description  |
|---|--|
| <code>&lt;log-message-string&gt;</code> | A string or a regular expression (PCRE) to match a log message or part of a log message. |

**Default** There is no type or log message string set by default.

**Mode** Trigger Configuration

**Usage notes** Log type triggers fully support regular expressions using PCRE (Perl-Compatible Regular Expression) syntax.

Only log messages of severity level notice or higher can activate a trigger.

Note that any command executed by the script will generate a log message with level notice, and will include '[SCRIPT]' before the command string. Therefore, if something in the script matches the configured log message trigger string, it will retrigger indefinitely.

**Example** To configure trigger 6 to activate when a log message of level notice or higher indicates that any port has 'failed', use the commands:

```
awplus# configure terminal
awplus(config)# trigger 6
awplus(config-trigger)# type log port.+ failed
```

**Related commands** [show trigger](#)  
[trigger](#)

**Command changes** Version 5.4.7-2.1: command added

# type memory

**Overview** This command configures a trigger to activate based on RAM usage level. Selecting the **up** option causes the trigger to activate when memory usage exceeds the specified level. Selecting the **down** option causes the trigger to activate when memory usage drops below the specified level. Selecting **any** causes the trigger to activate in both situations. The default is **any**.

**Syntax** `type memory <1-100> [up|down|any]`

| Parameter | Description  |
|-----------|--|
| <1-100>   | The percentage of memory usage at which to trigger.                        |
| up        | Activate when memory usage exceeds the specified level.                    |
| down      | Activate when memory usage drops below the specified level.                |
| any       | Activate when memory usage passes the specified level in either direction. |

**Mode** Trigger Configuration

**Examples** To configure trigger 12 to be a memory trigger that activates when memory usage exceeds 50% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# type memory 50 up
```

To configure trigger 40 to be a memory trigger that activates when memory usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65
```

or

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65 any
```

**Related commands** [show trigger](#)  
[trigger](#)

# type periodic

**Overview** This command configures a trigger to be activated at regular intervals. The time period between activations is specified in minutes.

**Syntax** `type periodic <1-1440>`

| Parameter                   | Description                                |
|-----------------------------|--|
| <code>&lt;1-1440&gt;</code> | The number of minutes between activations. |

**Mode** Trigger Configuration

**Usage notes** A combined limit of 10 triggers of the type periodic and time can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or periodic
```

For an example trigger configuration that uses the **type periodic** command, see "See Daily Statistics" in the [Triggers\\_Feature Overview and Configuration Guide](#).

**Example** To configure trigger 44 to activate periodically at 10 minute intervals use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 44
awplus(config-trigger)# type periodic 10
```

**Related commands** [show trigger](#)  
[trigger](#)

# type ping-poll

**Overview** This command configures a trigger that activates when Ping Polling identifies that a target device's status has changed. This allows you to run a configuration script when a device becomes reachable or unreachable.

**Syntax** `type ping-poll <1-100> {up|down}`

| Parameter | Description   |
|-----------|---|
| <1-100>   | The ping poll ID.   |
| up        | The trigger activates when ping polling detects that the target is reachable.   |
| down      | The trigger activates when ping polling detects that the target is unreachable. |

**Mode** Trigger Configuration

**Example** To configure trigger 106 to activate when ping poll 12 detects that its target device is now unreachable, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 106
awplus(config-trigger)# type ping-poll 12 down
```

**Related commands** [show trigger](#)  
[trigger](#)



# type reboot

**Overview** This command configures a trigger that activates when your device is rebooted.

**Syntax** type reboot

**Mode** Trigger Configuration

**Example** To configure trigger 32 to activate when your device reboots, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 32
awplus(config-trigger)# type reboot
```

**Related commands** [show trigger](#)  
[trigger](#)

# type time

**Overview** This command configures a trigger that activates at a specified time of day.

**Syntax** `type time <hh:mm>`

| Parameter                  | Description                       |
|----------------------------|-----------------------------------|
| <code>&lt;hh:mm&gt;</code> | The time to activate the trigger. |

**Mode** Trigger Configuration

**Usage** A combined limit of 10 triggers of the type time and type periodic can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or
periodic
```

**Example** To configure trigger 86 to activate at 15:53, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type time 15:53
```

**Related commands** [show trigger](#)  
[trigger](#)

# type usb

**Overview** Use this command to configure a trigger that activates on either the removal or the insertion of a USB storage device.

**Syntax** `type usb {in|out}`

| Parameter | Description   |
|-----------|---|
| in        | Trigger activates on insertion of a USB storage device. |
| out       | Trigger activates on removal of a USB storage device.   |

**Mode** Trigger Configuration

**Usage notes** USB triggers cannot execute script files from a USB storage device.

**Examples** To configure trigger 1 to activate on the insertion of a USB storage device, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 1
awplus(config-trigger)# type usb in
```

**Related commands** [trigger](#)  
[show running-config trigger](#)  
[show trigger](#)

# undebbug trigger

**Overview** This command applies the functionality of the **no debug trigger** command.

# 27

# Ping-Polling Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure Ping Polling. For more information, see the [Ping Polling Feature Overview and Configuration Guide](#).

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Table 27-1: The following table lists the default values when configuring a ping poll

| Default           | Value   |
|-------------------|---|
| Critical-interval | 1 second  |
| Description       | No description  |
| Fail-count        | 5   |
| Length            | 32 bytes  |
| Normal-interval   | 30 seconds  |
| Sample-size       | 5   |
| Source-ip         | The IP address of the interface from which the ping packets are transmitted |
| Time-out          | 1 second  |
| Up-count          | 30  |

- Command List**
- [“active \(ping-polling\)”](#) on page 1191
  - [“clear ping-poll”](#) on page 1192
  - [“critical-interval”](#) on page 1193
  - [“debug ping-poll”](#) on page 1194

- [“description \(ping-polling\)”](#) on page 1195
- [“fail-count”](#) on page 1196
- [“ip \(ping-polling\)”](#) on page 1197
- [“length \(ping-poll data\)”](#) on page 1198
- [“normal-interval”](#) on page 1199
- [“ping-poll”](#) on page 1200
- [“sample-size”](#) on page 1201
- [“show counter ping-poll”](#) on page 1203
- [“show ping-poll”](#) on page 1205
- [“source-ip”](#) on page 1209
- [“timeout \(ping polling\)”](#) on page 1211
- [“up-count”](#) on page 1212
- [“undebug ping-poll”](#) on page 1213

# active (ping-polling)

**Overview** This command enables a ping-poll instance. The polling instance sends ICMP echo requests to the device with the IP address specified by the [ip \(ping-polling\)](#) command.

By default, polling instances are disabled. When a polling instance is enabled, it assumes that the device it is polling is unreachable.

The **no** variant of this command disables a ping-poll instance. The polling instance no longer sends ICMP echo requests to the polled device. This also resets all counters for this polling instance.

**Syntax** active  
no active

**Mode** Ping-Polling Configuration

**Examples** To activate the ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# active
```

To disable the ping-poll instance 43 and reset its counters, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no active
```

**Related commands** [debug ping-poll](#)  
[ip \(ping-polling\)](#)  
[ping-poll](#)  
[show ping-poll](#)

# clear ping-poll

**Overview** This command resets the specified ping poll, or all ping poll instances. This clears the ping counters, and changes the status of polled devices to unreachable. The polling instance changes to the polling frequency specified with the [critical-interval](#) command. The device status changes to reachable once the device responses have reached the [up-count](#).

**Syntax** `clear ping-poll {<1-100>|all}`

| Parameter | Description  |
|-----------|--|
| <1-100>   | A ping poll ID number. The specified ping poll instance has its counters cleared, and the status of the device it polls is changed to unreachable. |
| all       | Clears the counters and changes the device status of all polling instances.  |

**Mode** Privileged Exec

**Examples** To reset the ping poll instance 12, use the command:

```
awplus# clear ping-poll 12
```

To reset all ping poll instances, use the command:

```
awplus# clear ping-poll all
```

**Related commands**

- [active \(ping-polling\)](#)
- [ping-poll](#)
- [show ping-poll](#)



# critical-interval

**Overview** This command specifies the time period in seconds between pings when the polling instance has not received a reply to at least one ping, and when the device is unreachable.

This command enables the device to quickly observe changes in state, and should be set to a much lower value than the [normal-interval](#) command.

The **no** variant of this command sets the critical interval to the default of one second.

**Syntax** `critical-interval <1-65536>`  
`no critical-interval`

| Parameter                    | Description  |
|------------------------------|--|
| <code>&lt;1-65536&gt;</code> | Time in seconds between pings, when the device has failed to a ping, or the device is unreachable. |

**Default** The default is 1 second.

**Mode** Ping-Polling Configuration

**Examples** To set the critical interval to 2 seconds for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# critical-interval 2
```

To reset the critical interval to the default of one second for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# no critical-interval
```

**Related commands**

[fail-count](#)  
[normal-interval](#)  
[sample-size](#)  
[show ping-poll](#)  
[timeout \(ping polling\)](#)  
[up-count](#)

# debug ping-poll

**Overview** This command enables ping poll debugging for the specified ping-poll instance. This generates detailed messages about ping execution.

The **no** variant of this command disables ping-poll debugging for the specified ping-poll.

**Syntax** `debug ping-poll <1-100>`  
`no debug ping-poll {<1-100>|all}`

| Parameter | Description                       |
|-----------|-----------------------------------|
| <1-100>   | A unique ping poll ID number.     |
| all       | Turn off all ping-poll debugging. |

**Mode** Privileged Exec

**Examples** To enable debugging for ping-poll instance 88, use the command:

```
awplus# debug ping-poll 88
```

To disable all ping poll debugging, use the command:

```
awplus# no debug ping-poll all
```

To disable debugging for ping-poll instance 88, use the command:

```
awplus# no debug ping-poll 88
```

**Related commands**

- [active \(ping-polling\)](#)
- [clear ping-poll](#)
- [ping-poll](#)
- [show ping-poll](#)
- [undebug ping-poll](#)

# description (ping-polling)

**Overview** This command specifies a string to describe the ping-polling instance. This allows the ping-polling instance to be recognized easily in show commands. Setting this command is optional.

By default ping-poll instances do not have a description.

Use the **no** variant of this command to delete the description set.

**Syntax** `description <description>`  
`no description`

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;description&gt;</code> | The description of the target. Valid characters are any printable character and spaces. There is no maximum character length. |

**Mode** Ping-Polling Configuration

**Examples** To add the text "Primary Gateway" to describe the ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# description Primary Gateway
```

To delete the description set for the ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no description
```

**Related commands** [ping-poll](#)  
[show ping-poll](#)

# fail-count

**Overview** This command specifies the number of pings that must be unanswered, within the total number of pings specified by the [sample-size](#) command, for the ping-polling instance to consider the device unreachable.

If the number set by the [sample-size](#) command and the **fail-count** commands are the same, then the unanswered pings must be consecutive. If the number set by the [sample-size](#) command is greater than the number set by the **fail-count** command, then a device that does not always reply to pings may be declared unreachable.

The **no** variant of this command resets the fail count to the default.

**Syntax** `fail-count <1-100>`  
`no fail-count`

| Parameter                  | Description  |
|----------------------------|--|
| <code>&lt;1-100&gt;</code> | The number of pings within the sample size that a reachable device must fail to respond to before it is classified as unreachable. |

**Default** The default is 5.

**Mode** Ping-Polling Configuration

**Examples** To specify the number of pings that must fail within the sample size to determine that a device is unreachable for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# fail-count 5
```

To reset the fail-count to its default of 5 for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no fail-count
```

**Related commands**

- [critical-interval](#)
- [normal-interval](#)
- [ping-poll](#)
- [sample-size](#)
- [show ping-poll](#)
- [timeout \(ping polling\)](#)
- [up-count](#)

# ip (ping-polling)

**Overview** This command specifies the IPv4 address of the device you are polling.

**Syntax** `ip {<ip-address>|<ipv6-address>}`

| Parameter                         | Description  |
|-----------------------------------|--|
| <code>&lt;ip-address&gt;</code>   | An IPv4 address in dotted decimal notation A.B.C.D |
| <code>&lt;ipv6-address&gt;</code> | An IPv6 address in hexadecimal notation X:X::X:X   |

**Mode** Ping-Polling Configuration

**Examples** To set ping-poll instance 5 to poll the device with the IP address 192.168.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 5
awplus(config-ping-poll)# ip 192.168.0.1
```

To set ping-poll instance 10 to poll the device with the IPv6 address 2001:db8::, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 10
awplus(config-ping-poll)# ip 2001:db8::
```

**Related commands**

- [ping-poll](#)
- [source-ip](#)
- [show ping-poll](#)

# length (ping-poll data)

**Overview** This command specifies the number of data bytes to include in the data portion of the ping packet. This allows you to set the ping packets to a larger size if you find that larger packet types in your network are not reaching the polled device, while smaller packets are getting through. This encourages the polling instance to change the device's status to unreachable when the network is dropping packets of the size you are interested in.

The **no** variant of this command resets the data bytes to the default of 32 bytes.

**Syntax** length <4-1500>  
no length

| Parameter | Description   |
|-----------|---|
| <4-1500>  | The number of data bytes to include in the data portion of the ping packet. |

**Default** The default is 32.

**Mode** Ping-Polling Configuration

**Examples** To specify that ping-poll instance 12 sends ping packet with a data portion of 56 bytes, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 12
awplus(config-ping-poll)# length 56
```

To reset the number of data bytes in the ping packet to the default of 32 bytes for ping-poll instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 12
awplus(config-ping-poll)# length
```

**Related commands** ping-poll  
show ping-poll

# normal-interval

**Overview** This command specifies the time period between pings when the device is reachable.

The **no** variant of this command resets the time period to the default of 30 seconds.

**Syntax** `normal-interval <1-65536>`  
`no normal-interval`

| Parameter                    | Description   |
|------------------------------|---|
| <code>&lt;1-65536&gt;</code> | Time in seconds between pings when the target is reachable. |

**Default** The default is 30 seconds.

**Mode** Ping-Polling Configuration

**Examples** To specify a time period of 60 seconds between pings when the device is reachable for ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# normal-interval 60
```

To reset the interval to the default of 30 seconds for ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no normal-interval
```

**Related commands**

- [critical-interval](#)
- [fail-count](#)
- [ping-poll](#)
- [sample-size](#)
- [show ping-poll](#)
- [timeout \(ping polling\)](#)
- [up-count](#)

# ping-poll

**Overview** This command enters the ping-poll configuration mode. If a ping-poll exists with the specified number, then this command enters its configuration mode. If no ping-poll exists with the specified number, then this command creates a new ping poll with this ID number.

To configure a ping-poll, create a ping poll using this command, and use the [ip \(ping-polling\)](#) command to specify the device you want the polling instance to poll. It is not necessary to specify any further commands unless you want to change a command's default.

The **no** variant of this command deletes the specified ping poll.

**Syntax** `ping-poll <1-100>`  
`no ping-poll <1-100>`

| Parameter | Description                   |
|-----------|-------------------------------|
| <1-100>   | A unique ping poll ID number. |

**Mode** Global Configuration

**Examples** To create ping-poll instance 3 and enter ping-poll configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 3
awplus(config-ping-poll)#
```

To delete ping-poll instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# no ping-poll 3
```

**Related commands**

- [active \(ping-polling\)](#)
- [clear ping-poll](#)
- [debug ping-poll](#)
- [description \(ping-polling\)](#)
- [ip \(ping-polling\)](#)
- [length \(ping-poll data\)](#)
- [show ping-poll](#)
- [source-ip](#)



# sample-size

**Overview** This command sets the total number of pings that the polling instance inspects when determining whether a device is unreachable. If the number of pings specified by the **fail-count** command go unanswered within the inspected sample, then the device is declared unreachable.

If the numbers set in this command and **fail-count** command are the same, the unanswered pings must be consecutive. If the number set by this command is greater than that set with the **fail-count** command, a device that does not always reply to pings may be declared unreachable.

You cannot set this command's value lower than the **fail-count** value.

The polling instance uses the number of pings specified by the **up-count** command to determine when a device is reachable.

The **no** variant of this command resets this command to the default.

**Syntax** `sample-size <1-100>`  
`no sample size`

| Parameter | Description   |
|-----------|---|
| <1-100>   | Number of pings that determines critical and up counts. |

**Default** The default is 5.

**Mode** Ping-Polling Configuration

**Examples** To set the sample-size to 50 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# sample-size 50
```

To reset sample-size to the default of 5 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no sample-size
```

**Related  
commands**

- critical-interval
- fail-count
- normal-interval
- ping-poll
- show ping-poll
- timeout (ping polling)
- up-count

# show counter ping-poll

**Overview** This command displays the counters for ping polling.

**Syntax** show counter ping-poll [*<1-100>*]

| Parameter            | Description   |
|----------------------|---|
| <i>&lt;1-100&gt;</i> | 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 27-1: Example output from the **show counter ping-poll** command

```
Ping-polling counters
Ping-poll: 1
PingsSent          ..... 15
PingsFailedUpState ..... 0
PingsFailedDownState ..... 0
ErrorSendingPing   ..... 2
CurrentUpCount     ..... 13
CurrentFailCount   ..... 0
UpStateEntered     ..... 0
DownStateEntered   ..... 0

Ping-poll: 2
PingsSent          ..... 15
PingsFailedUpState ..... 0
PingsFailedDownState ..... 0
ErrorSendingPing   ..... 2
CurrentUpCount     ..... 13
CurrentFailCount   ..... 0
UpStateEntered     ..... 0
DownStateEntered   ..... 0

Ping-poll: 5
PingsSent          ..... 13
PingsFailedUpState ..... 0
PingsFailedDownState ..... 2
ErrorSendingPing   ..... 2
CurrentUpCount     ..... 9
CurrentFailCount   ..... 0
UpStateEntered     ..... 0
DownStateEntered   ..... 0
```

**Table 28:** Parameters in output of the **show counter ping-poll** command

| Parameter            | Description  |
|----------------------|--|
| Ping-poll            | The ID number of the polling instance.   |
| PingsSent            | The total number of pings generated by the polling instance.   |
| PingsFailedUpState   | The number of unanswered pings while the target device is in the Up state. This is a cumulative counter for multiple occurrences of the Up state.            |
| PingsFailedDownState | Number of unanswered pings while the target device is in the Down state. This is a cumulative counter for multiple occurrences of the Down state.            |
| ErrorSendingPing     | The number of pings that were not successfully sent to the target device.<br>This error can occur when your device does not have a route to the destination. |
| CurrentUpCount       | The current number of sequential ping replies.   |
| CurrentFailCount     | The number of ping requests that have not received a ping reply in the current sample-size window.   |
| UpStateEntered       | Number of times the target device has entered the Up state.  |
| DownStateEntered     | Number of times the target device has entered the Down state.  |

**Example** To display counters for the polling instances, use the command:

```
awplus# show counter ping-poll
```

**Related commands**

- [debug ping-poll](#)
- [ping-poll](#)
- [show ping-poll](#)

# show ping-poll

**Overview** This command displays the settings and status of ping polls.

**Syntax** `show ping-poll [<1-100>|state {up|down}] [brief]`

| Parameter | Description  |   |
|-----------|--|---|
| <1-100>   | Displays settings and status for the specified polling instance.   |   |
| state     | Displays polling instances based on whether the device they are polling is currently reachable or unreachable. |   |
|           | up   | Displays polling instance where the device state is reachable.    |
|           | down   | Displays polling instances where the device state is unreachable. |
| brief     | Displays a summary of the state of ping polls, and the devices they are polling.                               |   |

**Mode** User Exec and Privileged Exec

**Output** Figure 27-2: 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 29:** Parameters in output of the **show ping-poll brief** command

| Parameter | Meaning  |
|-----------|--|
| Id        | The ID number of the polling instance, set when creating the polling instance with the <code>ping-poll</code> command. |
| Enabled   | Whether the polling instance is enabled or disabled.   |

**Table 29:** Parameters in output of the **show ping-poll brief** command (cont.)

| Parameter     | Meaning  |
|---------------|--|
| State         | The current status of the device being polled:   |
| Up            | The device is reachable.   |
| Down          | The device is unreachable.   |
| Critical Up   | The device is reachable but recently the polling instance has not received some ping replies, so the polled device may be going down.    |
| Critical Down | The device is unreachable but the polling instance received a reply to the last ping packet, so the polled device may be coming back up. |
| Destination   | The IP address of the polled device, set with the <code>ip (ping-polling)</code> command.  |

**Figure 27-3:** 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 30:** Parameters in output of the **show ping-poll** command

| Parameter              | Description   |   |
|------------------------|---|---|
| Description            | Optional description set for the polling instance with the <a href="#">description (ping-polling)</a> command.  |   |
| Destination IP address | The IP address of the polled device, set with the <a href="#">ip (ping-polling)</a> command.  |   |
| Status                 | The current status of the device being polled:  |   |
|                        | Up  | The device is reachable.  |
|                        | Down  | The device is unreachable.  |
|                        | Critical Up   | The device is reachable but recently the polling instance has not received some ping replies, so the polled device may be going down. |
| Critical Down          | The device is unreachable but the polling instance received a reply to the last ping packet, so the polled device may be coming back up.  |   |
| Enabled                | Whether the polling instance is enabled or disabled. The <a href="#">active (ping-polling)</a> and <a href="#">active (ping-polling)</a> commands enable and disable a polling instance.                              |   |
| Source IP address      | The source IP address sent in the ping packets. This is set using the <a href="#">source-ip</a> command.  |   |
| Critical interval      | The time period in seconds between pings when the polling instance has not received a reply to at least one ping, and when the device is unreachable. This is set with the <a href="#">critical-interval</a> command. |   |
| Normal interval        | The time period between pings when the device is reachable. This is set with the <a href="#">normal-interval</a> command.   |   |

**Table 30:** Parameters in output of the **show ping-poll** command (cont.)

| Parameter   | Description  |
|-------------|--|
| Fail count  | The number of pings that must be unanswered, within the total number of pings specified by the <a href="#">sample-size</a> command, for the polling instance to consider the device unreachable. This is set using the <a href="#">fail-count</a> command. |
| Up count    | The number of consecutive pings that the polling instance must receive a reply to before classifying the device reachable again. This is set using the <a href="#">up-count</a> command.   |
| Sample size | The total number of pings that the polling instance inspects when determining whether a device is unreachable. This is set using the <a href="#">sample-size</a> command.  |
| Length      | The number of data bytes to include in the data portion of the ping packet. This is set using the <a href="#">length (ping-poll data)</a> command.   |
| Timeout     | The time in seconds that the polling instance waits for a response to a ping packet. This is set using the <a href="#">timeout (ping polling)</a> command.   |
| Debugging   | Indicates whether ping polling debugging is <b>Enabled</b> or <b>Disabled</b> . This is set using the <a href="#">debug ping-poll</a> command.   |

**Examples** To display the ping poll settings and the status of all the polls, use the command:

```
awplus# show ping-poll
```

To display a summary of the ping poll settings, use the command:

```
awplus# show ping-poll brief
```

To display the settings for ping poll 6, use the command:

```
awplus# show ping-poll 6
```

To display a summary of the state of ping poll 6, use the command:

```
awplus# show ping-poll 6 brief
```

To display the settings of ping polls that have reachable devices, use the command:

```
awplus# show ping-poll state up
```

To display a summary of ping polls that have unreachable devices, use the command:

```
awplus# show ping-poll state down brief
```

**Related commands** [debug ping-poll](#)  
[ping-poll](#)



# source-ip

**Overview** This command specifies the source IP address to use in ping packets.

By default, the polling instance uses the address of the interface through which it transmits the ping packets. It uses the device's local interface IP address when it is set. Otherwise, the IP address of the interface through which it transmits the ping packets is used.

The **no** variant of this command resets the source IP in the packets to the device's local interface IP address.

**Syntax** `source-ip {<ip-address>|<ipv6-address>}`  
`no source-ip`

| Parameter                         | Description  |
|-----------------------------------|--|
| <code>&lt;ip-address&gt;</code>   | An IPv4 address in dotted decimal notation A.B.C.D |
| <code>&lt;ipv6-address&gt;</code> | An IPv6 address in hexadecimal notation X:X::X:X   |

**Mode** Ping-Polling Configuration

**Examples** To configure the ping-polling instance 43 to use the source IP address 192.168.0.1 in ping packets, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# source-ip 192.168.0.1
```

To configure the ping-polling instance 43 to use the source IPv6 address 2001:db8:: in ping packets, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# source-ip 2001:db8::
```

To reset the source IP address to the device's local interface IP address for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no source-ip
```

**Related commands**

- description (ping-polling)
- ip (ping-polling)
- length (ping-poll data)
- ping-poll
- show ping-poll

# timeout (ping polling)

**Overview** This command specifies the time in seconds that the polling instance waits for a response to a ping packet. You may find a higher time-out useful in networks where ping packets have a low priority.

The **no** variant of this command resets the set time out to the default of one second.

**Syntax** `timeout <1-30>`  
`no timeout`

| Parameter | Description  |
|-----------|--|
| <1-30>    | Length of time, in seconds, that the polling instance waits for a response from the polled device. |

**Default** The default is 1 second.

**Mode** Ping-Polling Configuration

**Examples** To specify the timeout as 5 seconds for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# timeout 5
```

To reset the timeout to its default of 1 second for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no timeout
```

**Related commands**

- [critical-interval](#)
- [fail-count](#)
- [normal-interval](#)
- [ping-poll](#)
- [sample-size](#)
- [show ping-poll](#)
- [up-count](#)

# up-count

**Overview** This command sets the number of consecutive pings that the polling instance must receive a reply to before classifying the device reachable again.

The **no** variant of this command resets the up count to the default of 30.

**Syntax** `up-count <1-100>`  
`no up-count`

| Parameter                  | Description  |
|----------------------------|--|
| <code>&lt;1-100&gt;</code> | Number of replied pings before an unreachable device is classified as reachable. |

**Default** The default is 30.

**Mode** Ping-Polling Configuration

**Examples** To set the upcount to 5 consecutive pings for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# up-count 5
```

To reset the upcount to the default value of 30 consecutive pings for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no up-count
```

**Related commands**

- [critical-interval](#)
- [fail-count](#)
- [normal-interval](#)
- [ping-poll](#)
- [sample-size](#)
- [show ping-poll](#)
- [timeout \(ping polling\)](#)

# undebug ping-poll

**Overview** This command applies the functionality of the no `debug ping-poll` command.

# Part 6: Firewall and Network Address Translation (NAT)

# 28

# Firewall Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure AlliedWare Plus Firewall. For more information see the [Firewall\\_and Network Address Translation \(NAT\) Feature Overview and Configuration\\_Guide](#).

The table below lists the firewall commands and their applicable modes.

Figure 28-1: Firewall commands and applicable modes

| Mode                   | Command                                      |
|------------------------|--|
| Privileged Exec        | <code>clear firewall connections</code>      |
|                        | <code>debug firewall</code>                  |
|                        | <code>show debugging firewall</code>         |
|                        | <code>show firewall</code>                   |
|                        | <code>show firewall connections</code>       |
|                        | <code>show firewall rule</code>              |
|                        | <code>show firewall rule config-check</code> |
|                        | <code>show running-config firewall</code>    |
| Global Configuration   | <code>firewall</code>                        |
| Firewall Configuration | <code>protect (firewall)</code>              |
|                        | <code>rule (firewall)</code>                 |
|                        | <code>move rule (firewall)</code>            |

- Command List**
- “[clear firewall connections](#)” on page 1217
  - “[connection-limit \(firewall\)](#)” on page 1218
  - “[connection-log events](#)” on page 1219

- [“firewall”](#) on page 1220
- [“debug firewall”](#) on page 1221
- [“ip tcp timeout established”](#) on page 1222
- [“move rule \(firewall\)”](#) on page 1223
- [“protect \(firewall\)”](#) on page 1224
- [“rule \(firewall\)”](#) on page 1225
- [“show connection-log events”](#) on page 1227
- [“show firewall”](#) on page 1228
- [“show firewall connections”](#) on page 1229
- [“show firewall connections limits”](#) on page 1230
- [“show firewall connections limits config-check”](#) on page 1231
- [“show firewall rule”](#) on page 1232
- [“show firewall rule config-check”](#) on page 1234
- [“show debugging firewall”](#) on page 1235
- [“show running-config firewall”](#) on page 1236



# clear firewall connections

**Overview** Use this command to clear firewall connections.

**Syntax** `clear firewall connections`

**Mode** Privileged Exec

**Usage notes** Removing the Network Address Translation (NAT) rule by using the **no nat rule** command for an actively translated flow does not stop translating immediately. This means subsequent packets in the flow are continued to be translated.

The continued translation after associated NAT rule is removed will only stop when:

- You use the **clear firewall connections** command to manually stop translations immediately, when the associated rule has been deleted regardless whether the firewall feature is actually configured with NAT or not.
- The traffic flow ends naturally, for example, when it is stopped from the source. If the flow is re-initiated from a host, it will not be translated by the firewall, as the rule is deleted after the first flow stopped.

**Examples** To clear firewall connections, use the command:

```
awplus# clear firewall connections
```

**Validation commands** [show firewall connections](#)

**Related commands** [rule \(nat\)](#)

# connection-limit (firewall)

**Overview** Use this command to limit firewall connections for an entity.

Use the **no** variant of this command to remove the limit.

**Syntax** `connection-limit [<1-65535>] from <entity_name> with limit <0-100000>`  
`no connection-limit {<1-65535>|all}`

| Parameter     | Description   |
|---------------|---|
| <1-65535>     | Unique numeric identifier for the limit.  |
| <entity_name> | An entity represents a logical grouping of subnets, hosts or interfaces. For more information about entity, see the <a href="#">Application and Entity Commands</a> . |
| <0-100000>    | The maximum number of permitted connections for the entity.   |
| all           | Delete all limits.  |

**Default** The limiting is disabled by default and the number of connections will not be limited. However, the number is up to the maximum total number of allowed connections.

**Mode** Firewall Configuration

**Usage notes** This command allows you to limit the number of firewall sessions associated with a specific entity. The limit will be applied to each host on that entity. This means connection limits applied to an entity with multiple addresses will apply the limit to individual hosts, not the total connections for the entity. The limit applies to both IPv4 and IPv6.

If a connection limit rule is removed, any running connections are not stopped. Changes to limits only affect new connections. Adding a lower limit will not affect existing connections.

**Examples** To set a connection limit for entity DMZ, use the following command:

```
awplus(config-firewall)# connection-limit  
1 from DMZ with limit 10000
```

To remove the connection limit, use the following command:

```
awplus(config-firewall)# no connection-limit  
1
```

**Validation commands** [show firewall connections](#)  
[show firewall connections limits](#)

# connection-log events

**Overview** Use this command to enable extra logging for indicating the start and the end of connections passing through the firewall.

Use the **no** variant of this command to turn off the extra logging of connections passing through the firewall.

**Syntax** `connection-log events [new|end|all]`  
`no connection-log events [new|end|all]`

| Parameter | Description  |
|-----------|--|
| new       | New connection                                       |
| end       | Connections closed                                   |
| all       | All new connections and connections closed. Default. |

**Default** Connection logging is not enabled by default.

**Mode** Global Configuration.

**Usage notes** There are two types of messages you can log: new connections and connections that ended. You can control the amount of messages you log by choosing to log either type of message or all of the message types.

Messages contain the following information:

- time
- source and destination addresses (NATed and unNATed)
- protocol
- source and destination ports (NATed and unNATed)
- bytes and packets passed (found in the connection end message)

**Example** To log all of the new connections and all of the closed connections, use the commands:

```
awplus# configure terminal
awplus(config)# connection-log events all
```

**Related commands** [show connection-log events](#)

**Command changes** Version 5.4.7-1.1: command added.

# firewall

**Overview** Use this command to configure the firewall.  
Use the **no** variant of this command to remove all firewall configuration.

**Syntax** `firewall`  
`no firewall`

**Mode** Global Configuration

**Usage notes** This command allows you to enter the Firewall Configuration mode. The command prompt for this mode is **awplus(config-firewall)#**

In the Firewall Configuration mode, you can:

- Enable or disable firewall protection, see the [protect \(firewall\)](#) command.
- Create, move, or delete rules for the firewall, see the [rule \(firewall\)](#) command and the [move rule \(firewall\)](#) command.

**Examples** To configure the firewall, use the commands:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)#
```

To remove all firewall configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no firewall
```

**Validation commands** `show firewall`  
`show running-config firewall`

# debug firewall

**Overview** Use this command to enable firewall debugging and Network Address Translation (NAT) debugging. This will cause additional detailed debugging information to be logged at the “informational” and “debugging” levels.

Use the **no** variant of this command to disable firewall debugging and NAT debugging.

For more information about NAT, see the [Firewall\\_and Network Address Translation \(NAT\) Feature Overview and Configuration\\_Guide](#).

**Syntax** debug firewall  
no debug firewall

**Default** Firewall debugging and NAT debugging are disabled by default.

**Mode** Privileged Exec

**Examples** To enable firewall debugging and NAT debugging, use the command:

```
awplus# debug firewall
```

To disable firewall debugging and NAT debugging, use the command:

```
awplus# no debug firewall
```

**Validation commands** [show debugging firewall](#)

# ip tcp timeout established

**Overview** Use this command to set the idle timeout for all established TCP connections. Use the **no** variant of this command to set the idle timeout back to the default of 3600 seconds.

**Syntax** `ip tcp timeout established <1-31536000>`  
`no ip tcp timeout established`

| Parameter                       | Description  |
|---------------------------------|--|
| <code>&lt;1-31536000&gt;</code> | Idle timeout for established TCP connections in seconds from 1 to 3153600. |

**Default** 3600 seconds (1 hour)

**Mode** Global Configuration

**Usage notes** By default, when a TCP session is successfully established through the firewall, when the session goes idle, it automatically times out of the firewall connection tracking table after 3600 seconds. In some situations it may be beneficial to time out unused established TCP sessions earlier.

For example, in a busy environment where there is an excessive number of sessions being established, the firewall connection tracking table could become oversubscribed, with new connections being blocked until older sessions are timed out.

**Example** To set a non-default TCP session timeout for established idle sessions of 1800 seconds (30 minutes), use the commands:

```
awplus# configure terminal
awplus(config)# ip tcp timeout established 1800
```

**Example** To set the TCP session timeout for established idle sessions back to the default setting of 3600 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip tcp timeout established
```

**Related commands** [show running-config](#)

**Command changes** Version 5.4.6-1.1: command added

# move rule (firewall)

**Overview** Use this command to change the order of firewall rules.

Firewall rules are applied in rule ID order. When rules match the same application, source entity and destination entity, only the rule with the lowest ID is applied.

Note that you can move an existing rule ID only to an ID that is not assigned to any rule; otherwise you will be given an error message. Also note that a change to the rule order may change the rule results.

**Syntax** `move rule <1-65535> to <1-65535>`

| Parameter                              | Description  |
|--|--|
| <code>move rule &lt;1-65535&gt;</code> | Move the ID of a given rule. The rule ID of the given rule must exist.<br>Each rule has an ID which is either designated by the user or automatically generated when the rule is created. The rule ID is an integer from 1 to 65535. |
| <code>to &lt;1-65535&gt;</code>        | New rule ID to assign. The new rule ID must not be used by any existing rule.  |

**Mode** Firewall Configuration

**Examples** To change the rule ID from 20 to 10, use the commands:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# move rule 20 to 10
```

**Validation commands** `show firewall rule`

`show running-config firewall`

**Related commands** `rule (firewall)`

# protect (firewall)

**Overview** Use this command to enable firewall protection.

Use the **no** variant of this command to disable firewall protection without losing the existing firewall configuration.

**Syntax** `protect`  
`no protect`

**Default** Firewall protection is disabled by default.

**Mode** Firewall Configuration

**Usage notes** Firewall protection is disabled by default and all traffic can pass through the firewall. When the firewall is enabled and no rules are added, all traffic will be blocked by default. You can use the [rule \(firewall\)](#) command to configure rules to allow traffic to pass through the firewall.

**Examples** To enable firewall protection, use the commands:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# protect
```

To disable firewall protection, use the commands:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# no protect
```

**Validation commands** [show firewall](#)  
[show running-config firewall](#)



# rule (firewall)

**Overview** Use this command to create a rule for the firewall. Firewall security policy is specified in the form of firewall rules. Each rule defines the appropriate processing of a type of traffic passing through the firewall.

Use the **no** variant of this command to remove a rule.

**Syntax** rule [*<1-65535>*] {permit|deny|reject|log} *<application-name>*  
from *<source-entity>* to *<destination-entity>*  
[no-state-enforcement] [log]  
no rule {*<1-65535>*|all}

| Parameter                         | Description   |
|-----------------------------------|---|
| <i>&lt;1-65535&gt;</i>            | Rule ID is an integer in the range <i>&lt;1-65535&gt;</i> . If you don't designate a rule ID, a rule ID will be automatically generated and it will be greater than the current highest rule ID.  |
| permit                            | Permit connections that match the application, source entity and destination entity specified with this command.  |
| deny                              | Drop connections that match the application, source entity and destination entity specified with this command. No error message is sent back to the source host.  |
| reject                            | Reject connections that match the application, source entity and destination entity specified with this command. An error message (for instance, a TCP reset for a rejected TCP connection, or a destination unreachable message for an ICMP connection, etc.) is sent back to the source host. |
| log                               | When 'log' is the action for the rule, log an event each time the rule is hit. The traffic will also be processed by subsequent firewall rules which may permit, deny or reject the connection.   |
| <i>&lt;application-name&gt;</i>   | Application name. You can either specify an application name or use the word <i>any</i> , which stands for all applications. For more information about applications, see Application and Entity Commands.  |
| <i>&lt;source-entity&gt;</i>      | Source entity name. An entity represents a logical grouping of subnets, hosts or interfaces. For more information about entities, see Application and Entity Commands.  |
| <i>&lt;destination-entity&gt;</i> | Destination entity name.  |

| Parameter            | Description   |
|----------------------|---|
| no-state-enforcement | Optionally disable state enforcement for this rule. Use this option with caution as it will allow reverse path connection initiation. It should be used only when the traffic forward and reverse paths must be different and there is no alternative approach available. This option is disabled by default. |
| log                  | When 'log' is appended to a rule, the action is applied and a log message is also generated each time the rule is hit.  |
| all                  | Delete all rules.   |

**Mode** Firewall Configuration

**Usage notes** When the firewall is enabled and no rules are added, all traffic is blocked by default, you can use this command to create rules for permitting packets between entities.

The rule is not valid and cannot be hit if either the application, source entity or destination entity the rule applies to is not properly configured, for example, the application does not exist or does not have a protocol configured or the entity does not exist. To configure applications and entities, see Application and Entity Commands. You can also use the [show firewall rule config-check](#) command to check rule configuration validity.

You can change the rule order by using the [move rule \(firewall\)](#) command.

**Examples** To create a rule for permitting application ping between 'public' and 'private', use the command:

```
awplus(config-firewall)# rule 10 permit
ping from public to private
```

To create a rule for denying application http between 'public.wan' and 'private.lan', use the command:

```
awplus(config-firewall)# rule 20 deny
http from public.wan to private.lan
```

To create a firewall rule to permit application 'ping' between 'public' and 'dmz' entities and to log the results, use the commands:

```
awplus(config-firewall)# rule 30 permit
ping from public to dmz log
```

**Related commands**

- [move rule \(firewall\)](#)
- [show firewall rule](#)
- [show firewall rule config-check](#)

**Command changes** Version 5.4.7-0.1: **no-state-enforcement** option added.

# show connection-log events

**Overview** This command displays the configuration state (enabled or disabled) for the logging of connections passing through the firewall, as configured by the [connection-log events](#) command.

**Syntax** `show connection-log events`

**Mode** User Exec

**Example** To show the logging configuration state for the connections passing through the firewall, use the command:

```
awplus# show connection-log events
```

**Output** Figure 28-2: Example output from **show connection-log events**

```
awplus#show connection-log events
Log new connection events:      Disabled
Log connection end events:     Enabled
```

**Related commands** [connection-log events](#)

**Command changes** Version 5.4.7-1.1: command added.

# show firewall

**Overview** Use this command to show the protection state of the firewall and the number of active connections being handled by the firewall.

You can use the [protect \(firewall\)](#) command to enable firewall protection.

**Syntax** `show firewall`

**Mode** Privileged Exec

**Examples** To show the state of the firewall, use the command:

```
awplus# show firewall
```

**Output** Figure 28-3: Example output from the **show firewall** command

```
awplus#show firewall
Firewall protection is enabled
Active connections: 9
```

**Related commands** [protect \(firewall\)](#)

# show firewall connections

**Overview** Use this command to show the connections currently being tracked by the firewall.

**Syntax** show firewall connections

**Mode** Privileged Exec

**Examples** To show the connections currently being tracked by the firewall, use the command:

```
awplus# show firewall connections
```

**Output** Figure 28-4: Example output from the **show firewall connections** command

```
awplus#show firewall connections
tcp ESTABLISHED src=192.168.1.2 dst=172.16.1.2 sport=58616
dport=23 packets=16
bytes=867 src=172.16.1.2 dst=172.16.1.1 sport=23 dport=58616
packets=11 bytes=636
[ASSURED]
icmpv6 src=2001:db8::2 dst=2001:db8::1 type=128 code=0 id=1416
packets=34
bytes=3536 src=2001:db8::1 dst=2001:db8::2 type=129 code=0 id=1416
packets=34
bytes=3536
tcp TIME_WAIT src=2001:db8:1::2 dst=2001:db8:2::2 sport=42532
dport=80 packets=7
bytes=597 src=2001:db8:2::2 dst=2001:db8:1::2 sport=80 dport=42532
packets=5
bytes=651 [ASSURED]
tcp TIME_WAIT src=2001:db8:1::2 dst=2001:db8:2::2 sport=48740
dport=80 packets=5
bytes=564 src=2001:db8:2::2 dst=2001:db8:1::2 sport=80 dport=48740
packets=5
bytes=594 [ASSURED]
```

**Related commands** [clear firewall connections](#)

# show firewall connections limits

**Overview** Use this command to show the configured firewall connection-limits for a given entity.

**Syntax** `show firewall connections limits`

**Mode** Privileged Exec

**Examples** To show the information about all the firewall connection limits, use the command:

```
awplus# show firewall connections limits
```

**Output** Figure 28-5: Example output from the **show firewall connections limits** command

```
awplus#show firewall connections limits
```

| ID | Entity | Limit | Hit Count |
|----|--------|-------|-----------|
| 10 | DMZ    | 100   | 42        |

**Related commands** [show firewall connections limits config-check](#)

# show firewall connections limits config-check

**Overview** Use this command to check configuration validity of firewall connection limits.

An invalid rule will not be active and cannot be hit. This command also shows the reasons why a limit configuration is not valid.

**Syntax** `show firewall connections limits config-check`

**Mode** Privileged Exec

**Usage notes** Firewall limits are applied to entities only. A limit is not valid if the source entity (zone) is not configured properly. This command checks if the entity exists at all, and if it does it also checks if the entity (zone) has a valid subnet.

**Examples** To check configuration validity of connection-limit rules, use the command:

```
awplus# show firewall connections limits  
config-check
```

**Output** Figure 28-6: Example output from the **show firewall connections limits config-check** command on the console if rule configuration errors are detected. Connection-limit 10 uses an entity that exists; however no subnet has been specified. Connection-limit 20 uses an entity that doesn't exist.

```
awplus#show firewall connections limits config-check  
Connection-limit 10:  
  "From" entity has no subnet or host addresses  
Connection-limit 20:  
  "From" entity does not exist
```

**Output** Figure 28-7: Example output from the **show firewall connections limits config-check** command if all limit rules are valid

```
awplus#show firewall connection limits config-check  
All rules are valid
```

**Related commands** [show firewall connections limits](#)

# show firewall rule

**Overview** Use this command to show information about firewall rules.

**Syntax** show firewall rule [<1-65535>]

| Parameter | Description |
|-----------|-------------|
| <1-65535> | Rule ID     |

**Mode** Privileged Exec

**Examples** To show information about all firewall rules, use the command:

```
awplus# show firewall rule
```

**Output** Figure 28-8: Example output from the **show firewall rule** command

```
awplus#show firewall rule

[* = Rule is not valid - see "show firewall rule config-check"]
  ID    Action App      From      To
Hits
-----
-----
  10    permit ping     public    private
  0
  20    permit ping     public    dmz
  0
  40    permit ping     private   dmz
  0
 * 50    permit voice    public    private
  0
```

To show information about a specific firewall rule, use the command:

```
awplus# show firewall rule 10
```

**Output** Figure 28-9: Example output from the **show firewall rule** command

```
awplus#show firewall rule 10

[* = Rule is not valid - see "show firewall rule config-check"]
  ID    Action App      From      To
Hits
-----
-----
  10    permit ping     public    private
  0
```



| Output Parameter | Description   |
|------------------|---|
| *                | Indicates the rule is not valid and cannot be hit, see the <a href="#">show firewall rule config-check</a> command. |
| Action           | The rule action set by the <a href="#">rule (firewall)</a> command.   |
| App              | Application name.   |
| From             | Source entity.  |
| To               | Destination entity.   |
| Hits             | The number of times the firewall rule has been hit.   |

**Related commands** [rule \(firewall\)](#)

# show firewall rule config-check

**Overview** Use this command to check configuration validity of firewall rules.  
An invalid rule will not be active and cannot be hit. This command also shows the reasons why a rule is not valid.

**Syntax** `show firewall rule config-check`

**Mode** Privileged Exec

**Usage notes** Firewall rules are applied to applications and entities. A rule is not valid if either the application, source entity or destination entity the rule applies to is not configured properly.

To configure applications and entities, see Application and Entity Commands.

**Examples** To check configuration validity of firewall rules, use the command:

```
awplus# show firewall rule config-check
```

**Output** Figure 28-10: Example output from the **show firewall rule config-check** command if rule configuration errors are detected

```
awplus#show firewall rule config-check
Rule 10:
  Application does not have a protocol configured
  "From" entity does not exist
  "To" entity has no subnet or host addresses
```

**Output** Figure 28-11: Example output from the **show firewall rule config-check** command if all rules are valid

```
awplus#show firewall rule config-check
All rules are valid
```

**Related commands** [rule \(firewall\)](#)  
[show firewall rule](#)

# show debugging firewall

**Overview** Use this command to see what debugging is turned on for firewall and Network Address Translation (NAT).

You can use the [debug firewall](#) command to enable firewall and NAT debugging.

For more information about NAT, see the [Firewall\\_and Network Address Translation \(NAT\) Feature Overview and Configuration\\_Guide](#).

**Syntax** show debugging firewall

**Mode** Privileged Exec

**Examples** To show the firewall and NAT debugging status, use the command:

```
awplus# show debugging firewall
```

**Output** Figure 28-12: Example output from the **show debugging firewall** command

```
awplus#show debugging firewall
Firewall Debugging Status: on
```

**Related commands** [debug firewall](#)

# show running-config firewall

**Overview** Use this command to show the configuration commands that have been used to configure the firewall.

**Syntax** `show running-config firewall`

**Mode** Privileged Exec

**Examples** To show the configuration commands that have been used to configure the firewall, use the command:

```
awplus# show running-config firewall
```

**Output** Figure 28-13: Example output from the **show running-config firewall** command

```
awplus#show running-config firewall
firewall
  rule 10 permit ping from public to private
  protect
!
```

# 29

# Application and Entity Commands

## Introduction

This chapter provides an alphabetical reference of commands used to configure application and entity. For more information, see the [Firewall\\_and Network Address Translation \(NAT\) Feature Overview and Configuration\\_Guide](#).

The table below lists the application commands and their applicable modes.

Figure 29-1: Application commands and applicable modes

| Mode                 | Command                              |
|----------------------|--------------------------------------|
| Privileged Exec      | <code>show application</code>        |
|                      | <code>show application detail</code> |
| Global Configuration | <code>application</code>             |
| Application Mode     | <code>protocol</code>                |
|                      | <code>icmp-type</code>               |
|                      | <code>icmp-code</code>               |
|                      | <code>sport</code>                   |
|                      | <code>dport</code>                   |

The table below lists the entity commands and their applicable modes.

Figure 29-2: Entity commands

| Mode                 | Command                     |
|----------------------|-----------------------------|
| Privileged Exec      | <code>show entity</code>    |
| Global Configuration | <code>zone</code>           |
| Zone Mode            | <code>network (zone)</code> |

---

| Mode         | Command                          |
|--------------|----------------------------------|
| Network Mode | <code>ip subnet</code>           |
|              | <code>ipv6 subnet</code>         |
|              | <code>host (network)</code>      |
| Host Mode    | <code>ip address (host)</code>   |
|              | <code>ipv6 address (host)</code> |

- Command List**
- `"application"` on page 1239
  - `"dport"` on page 1241
  - `"dscp"` on page 1243
  - `"host (network)"` on page 1245
  - `"icmp-code"` on page 1247
  - `"icmp-type"` on page 1249
  - `"ip address (host)"` on page 1251
  - `"ip subnet"` on page 1253
  - `"ipv6 address (host)"` on page 1255
  - `"ipv6 subnet"` on page 1257
  - `"network (zone)"` on page 1259
  - `"protocol"` on page 1261
  - `"show application"` on page 1262
  - `"show application detail"` on page 1263
  - `"show entity"` on page 1264
  - `"sport"` on page 1267
  - `"zone"` on page 1269

# application

**Overview** Use this command to create or modify a custom application.

An application is a high level abstraction of application packets being transported by network traffic. Traffic matching for applications can be achieved by using several techniques, for example, matching packets to port numbers or searching for application signatures in flows of packets.

Use the **no** variant of this command to delete a custom application.

**Syntax** `application <application-name>`  
`no application <application-name>`

| Parameter                             | Description   |
|---------------------------------------|---|
| <code>&lt;application-name&gt;</code> | Application name.<br>You can use all alphanumeric ASCII characters, and the dash (-) and underscore (_) characters. The name can be 1 to 64 characters long. The application name is case-sensitive. If you create two application names with the same spelling but one in upper case and the other one in lower case, the last overwrites the first entry. |

**Mode** Global Configuration

**Usage notes** Use this command to enter the Application Configuration mode, to create a custom application or configure an existing application. You can configure the source port, destination port, protocol, ICMP code and ICMP type for the application. An application is invalid if its protocol, source or destination are not properly configured, for example, if the application has no protocol configured, or source and destination ports are applied to protocols that are not TCP, UDP or SCTP.

There are 40 predefined applications with protocols, source and destination ports.

You can change the protocol, source and destination ports of the predefined applications. You can only delete the predefined application when you change either its protocol, source or destination port.

Use the [show application](#) command to show all the custom and predefined applications.

**Examples** To create a custom application named 'isakmp', use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)#
```

To delete the custom application named 'isakmp', use the commands:

```
awplus# configure terminal  
awplus(config)# no application isakmp
```

**Related  
commands**

dport  
icmp-code  
icmp-type  
protocol  
show application  
sport



# dport

**Overview** Use this command to specify a destination port or port range for an application.

A port number is part of the addressing information used to identify a specific process to which a network message is to be forwarded between a sender and a receiver. For the full list of port numbers and their assignment, you can visit the Internet Assigned Numbers Authority (IANA) website at [www.iana.org](http://www.iana.org).

Use the **no** variant of this command to delete a port or a port range from an application. Note that the port or port range that you want to delete must match exactly the existing port or port range. You cannot remove a port range that is part of an existing port range.

**Syntax** `dport {<destination-port>|any|<start-range> to <end-range>}`  
`no dport {<destination-port>|any|<start-range> to <end-range>}`

| Parameter                             | Description   |
|---------------------------------------|---|
| <code>&lt;destination-port&gt;</code> | The destination port number, either TCP or UDP, specified as an integer in the range <1-65535>. |
| <code>any</code>                      | Any port number in the range <1-65535>. This equals to a range of 1 to 65535.                   |
| <code>&lt;start-range&gt;</code>      | Starting port number in the range <1-65535>.  |
| <code>to &lt;end-range&gt;</code>     | Ending port number in the range <1-65535> or max.   |

**Mode** Application Mode

**Usage notes** You can create more than one destination port number or port range for an application.

**Examples** To specify destination port 500 for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# dport 500
```

To specify destination port 500 and a range of ports for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# dport 500
awplus(config-application)# dport 60000 to max
```

To specify the destination port any (a port number range of 1-65535) for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# dport any
```

To remove destination port 500 from the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# no dport 500
```

To remove port **any** from the application isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# no dport 1 to 65535
```

**Related  
commands**

[application](#)  
[sport](#)  
[show application](#)

# dscp

**Overview** Use this command to specify one or more DSCP values used by an application.

Use the **no** variant of this command to remove one or more DSCP values from an application.

**Syntax** `dscp <dscp-list>`

`dscp {af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|ef|be}`

`dscp {cs0|cs1|cs2|cs3|cs4|cs5|cs6|cs7}`

`no dscp`

`no dscp <dscp-list>`

`no dscp {af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|ef|be}`

`no dscp {cs0|cs1|cs2|cs3|cs4|cs5|cs6|cs7}`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;dscp-list&gt;</code> | One or more DSCP values, in the range 0-63. Use spaces to separate values.   |
| <code>af11 ... be</code>       | One or more DSCP values specified according to the Assured Forwarding group, as defined in RFC 2597 and RFC 3260. See the table below for values. "ef" means expedited forwarding (DSCP 46) and "be" means best effort (DSCP 0). Voice traffic is typically given a value of ef. |
| <code>cs0 ... cs7</code>       | One or more DSCP values specified according to the Class Selector group. This is equivalent to TOS IP precedence values, so that CS0 is equivalent to an IP precedence value of 0, CS1 is equivalent to an IP precedence value of 1, and so on.                                  |

Table 29-1: Assured Forwarding (AF) behavior group

|                         | Class 1           | Class 2           | Class 3           | Class 4           |
|-------------------------|-------------------|-------------------|-------------------|-------------------|
| Low drop probability    | AF11<br>(DSCP 10) | AF21<br>(DSCP 18) | AF31<br>(DSCP 26) | AF41<br>(DSCP 34) |
| Medium drop probability | AF12<br>(DSCP 12) | AF22<br>(DSCP 20) | AF32<br>(DSCP 28) | AF42<br>(DSCP 36) |
| High drop probability   | AF13<br>(DSCP 14) | AF23<br>(DSCP 22) | AF33<br>(DSCP 30) | AF43<br>(DSCP 38) |

**Mode** Application Mode

**Usage notes** You can specify only one set of DSCP values for an application. The newly specified list will replace the existing one; it will not be added to the existing one.

**Example** To specify a DSCP of **ef** for the application named **voice**, use the commands:

```
awplus# configure terminal
awplus(config)# application voice
awplus(config-application)# dscp ef
```

To specify DSCPs of 12 and 13 for the application named **test**, use the commands:

```
awplus# configure terminal
awplus(config)# application test
awplus(config-application)# dscp 12 13
```

To remove DSCP12 from the application named **test**, use the commands:

```
awplus# configure terminal
awplus(config)# application test
awplus(config-application)# no dscp 12
```

To stop the application named **test** from using DSCP values, use the commands:

```
awplus# configure terminal
awplus(config)# application test
awplus(config-application)# no dscp
```

**Related commands**

- [application](#)
- [show application](#)
- [show application detail](#)

# host (network)

**Overview** Use this command to add a host to a network entity or to configure an existing host.

Host is a high level abstraction of a single node in a network. This is commonly used if a particular device, for example a server, has a static IP address that needs to be specified in a firewall policy.

Use the **no** variant of this command to remove a host from a network entity.

**Syntax** `host <host-name>`  
`no host <host-name>`

| Parameter                      | Description  |
|--------------------------------|--|
| <code>&lt;host-name&gt;</code> | Host name.<br>You can use all alphanumeric ASCII characters, and the dash (-) and underscore (_) characters. The name can be 1 to 64 characters in long. |

**Mode** Network Mode

**Usage notes** You can create multiple hosts for a network. A host entity is identified by its parent network using the dot notation, for example, `ZoneName.NetworkName.HostName`.

This commands allows you to enter the Host Mode with the prompt **awplus(config-host)#**. The Host Mode enables you to configure IPv4 address and IPv6 address for the host. For more information about host IPv4 address and IPv6 address, see [ip address \(host\)](#) command and [ipv6 address \(host\)](#) command respectively.

**Example** To create a host entity named `ftp` under network entity `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# host ftp
awplus(config-host)#
```

To remove host entity `ftp` and its IP address configuration from network entity `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# no host ftp
```

**Validation  
commands**    show entity

**Related  
commands**    ip address (host)  
                  ipv6 address (host)  
                  network (zone)

# icmp-code

**Overview** Use this command to configure an ICMP message code for an application.

ICMP has many messages that are identified by a “type” field and many of these ICMP types have a “code” field. Use the `icmp-type` command to specify the ICMP type. For the full list of the ICMP code assignments, you can visit the Internet Assigned Numbers Authority (IANA) website at [www.iana.org](http://www.iana.org).

Use the **no** variant of this command to restore the ICMP message code to its default, which is **any**.

**Syntax** `icmp-code {<code-number>|any}`  
`no icmp-code`

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;code-number&gt;</code> | Specify an ICMP message code number in the range of 0 to 255. |
| <code>any</code>                 | Any ICMP message code in the range of 0 to 255.               |

**Default** The default ICMP code number is **any**.

**Mode** Application Mode

**Usage notes** You should configure the ICMP code only for applications that use protocol ICMP. To configure the application protocol, see the `protocol` command.

You can specify only one ICMP message code for an application. The newly specified code will replace the previous one.

**Examples** To specify ICMP code 5 (redirect) for the application named `icmp`, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# icmp-code 5
```

To specify the ICMP code as **any** for the application named `icmp`, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# icmp-code any
```

To restore the ICMP message code to its default of **any** for the application named `icmp`, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# no icmp-code
```

**Related  
commands** application  
icmp-type  
protocol  
show application



# icmp-type

**Overview** Use this command to configure an ICMP message type for an application.

The ICMP protocol has many messages that are identified by a “type” field. For the full list of the ICMP type assignments, you can visit the Internet Assigned Numbers Authority (IANA) website at [www.iana.org](http://www.iana.org).

Use the **no** variant of this command to restore the ICMP message type to its default, which is **any**.

**Syntax** `icmp-type {<type-number>|any}`  
`no icmp-type`

| Parameter     | Description   |
|---------------|---|
| <type-number> | Specify an ICMP message type number in the range of 0 to 255. |
| any           | Any ICMP message type in the range of 0 to 255.               |

**Default** The default ICMP type is **any**.

**Mode** Application Mode

**Usage notes** You should configure the ICMP type only for applications that use protocol ICMP. To configure the application protocol, see the [protocol](#) command.

You can specify only one ICMP message type for an application. The newly specified type will replace the previous one.

**Examples** To specify ICMP message type 8 (echo) for the application named icmp, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# icmp-type 8
```

To specify the ICMP message type as **any** for the application named icmp, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# icmp-type any
```

To restore the ICMP message type to its default of **any** for the application named icmp, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# no icmp-type
```

**Related  
commands** application  
icmp-code  
network (zone)  
show application

# ip address (host)

**Overview** Use this command to assign an IPv4 address to a host entity.  
Use the **no** variant of this command to remove an IPv4 address from the host.

**Syntax**

```
ip address <ipv4-address>
ip address dynamic fqdn <domain_name>
ip address dynamic interface <interface_name>
no ip address <ipv4-address>
no ip address dynamic fqdn <domain_name>
no ip address dynamic interface <interface_name>
```

| Parameter        | Description   |
|------------------|---|
| <ipv4-address>   | The IPv4 address uses the format A.B.C.D.                     |
| dynamic          | Dynamic IP address, for example, obtained from a DHCP server. |
| <domain_name>    | The FQDN to resolve IP addresses for.                         |
| <interface_name> | Interface to acquire IP addresses from.                       |

**Mode** Host

**Usage notes** You can add multiple IP addresses to a host entity. If the IP address is not in the scope of any of its parent network's IPv4 subnets, a warning message will be given. Such an IP address is still acceptable because in the future the user may assign a network subnet that contains the host's IP address. Firewall policy rules will not apply to an IP address that is not in at least one of the network's subnets.

If you are adding an FQDN, DNS Relay cache and **ip domain-lookup via-relay** must be enabled for this command to work. DNS requests passing through the router are inspected for matching FQDNs. Because of this, the DNS cache is cleared when this command is entered so that the IP addresses can be picked up.

You can add multiple dynamic FQDNs for a host entity.

**Examples** To add an IP address to host ftp, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 192.168.1.0/24
awplus(config-network)# host ftp
awplus(config-host)# ip address 192.168.1.5
```

To add multiple IP addresses to host ftp, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 192.168.1.0/24
awplus(config-network)# host ftp
awplus(config-host)# ip address 192.168.1.8
awplus(config-host)# ip address 192.168.1.9
awplus(config-host)# ip address 192.168.1.10
```

To add the IPv4 addresses of the FQDN "google.com" to a zone, use the following commands:

```
awplus# configure terminal
awplus(config)# zone Public
awplus(config-zone)# network Router
awplus(config-network)# ip subnet 0.0.0.0/0
awplus(config-network)# host google
awplus(config-host)# ip address dynamic fqdn google.com
```

To remove an IP address from host ftp, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# host ftp
awplus(config-host)# no ip address 192.168.1.5
```

**Validation commands** [show entity](#)

**Related commands** [host \(network\)](#)  
[ip domain-lookup](#)

**Command changes** Version 5.4.8-1.1: FQDN parameter and output added

# ip subnet

**Overview** Use this command to add an IPv4 subnet to a network entity.  
Use the **no** variant of this command to remove a subnet from a network entity.

**Syntax** `ip subnet <ip-network/m> [interface <interface-name>]`  
`no ip subnet <ip-network/m> [interface <interface-name>]`

| Parameter                           | Description  |
|-------------------------------------|--|
| <code>&lt;ip-network/m&gt;</code>   | IP address of the network, entered in the form A.B.C.D/M. Dotted decimal notation followed by a forward slash, and then the subnet mask length.  |
| <code>interface</code>              | Specify an interface name. An interface may be specified to add a further restriction on the subnet. No interface configured indicates that any matching address from any interface is a member of this network. |
| <code>&lt;interface-name&gt;</code> | Interface name. Any AlliedWare Plus interface type (eth, vlan, ppp, tunnel, lo and so on). A warning message is given if the interface does not match an existing interface on the device.                       |

**Mode** Network Mode

**Usage notes** You can create multiple subnets to a network entity.

**Examples** To add a subnet to network `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 192.168.2.0/24
```

To add a subnet and an interface to network `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 192.168.2.0/24 interface eth1
```

To add multiple subnets to network servers, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 192.168.2.0/24 interface eth1
awplus(config-network)# ip subnet 10.1.0.0/16 interface eth1
```

To remove a subnet from network servers, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# no ip subnet 192.168.2.0/24
```

**Validation commands** [show entity](#)

**Related commands** [network \(zone\)](#)

# ipv6 address (host)

**Overview** Use this command to assign an IPv6 address to a host entity.  
Use the **no** variant of this command to remove an IPv6 address from an host entity.

**Syntax**

```
ipv6 address <ipv6-address>  
ipv6 address dynamic fqdn <domain_name>  
ipv6 address dynamic interface <interface_name>  
no ipv6 address <ipv6-address>  
no ipv6 address dynamic fqdn <domain_name>  
no ipv6 address dynamic interface <interface_name>
```

| Parameter        | Description   |
|------------------|---|
| <ipv6-address>   | The IPv6 address in the format x:x::x:x.                        |
| dynamic          | Dynamic IPv6 address, for example, obtained from a DHCP server. |
| <domain_name>    | The FQDN to resolve IP addresses for.                           |
| <interface_name> | Interface to acquire IP addresses from.                         |

**Mode** Host Mode

**Usage notes** You can add multiple IPv6 addresses to a host entity. If the IPv6 address is not in the scope of any of its parent network's IPv6 subnets, a warning message will be given. Such an IP address is still acceptable because in the future the user may assign a network subnet that contains the host's IPv6 address. Firewall policy rules will not apply to an IPv6 address that is not in at least one of the network's subnets.

If you are adding an FQDN, DNS Relay cache and **ip domain-lookup via-relay** must be enabled for this command to work. DNS requests passing through the router are inspected for matching FQDNs. Because of this, the DNS cache is cleared when this command is entered so that the IPv6 addresses can be picked up.

You can add multiple dynamic FQDNs for a host entity.

**Examples** To add an IPv6 address to host web-server, use the commands:

```
awplus# configure terminal  
awplus(config)# zone dmz  
awplus(config-zone)# network servers  
awplus(config-network)# ipv6 subnet 2001:db8:24:100::/64  
awplus(config-network)# host web-server  
awplus(config-host)# ipv6 address 2001:db8:24:100::1
```

To add multiple IP addresses to host `web-server`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ipv6 subnet 2001:db8:24:100::/64
awplus(config-network)# host web-server
awplus(config-host)# ipv6 address 2001:db8:24:100::2
awplus(config-host)# ipv6 address 2001:db8:24:100::3
awplus(config-host)# ipv6 address 2001:db8:24:100::4
```

To add the IPv6 addresses of the FQDN "google.com" to a zone, use the following commands:

```
awplus# configure terminal
awplus(config)# zone Public
awplus(config-zone)# network Router
awplus(config-network)# ip subnet ::/0
awplus(config-network)# host google
awplus(config-host)# ip address dynamic fqdn google.com
```

To remove an IPv6 address from host `web-server`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# host web-server
awplus(config-host)# no ipv6 address 2001:db8:24:100::2
```

**Validation commands** [show entity](#)

**Related commands** [host \(network\)](#)  
[ip domain-lookup](#)

**Command changes** Version 5.4.8-1.1: FQDN parameter and output added



# ipv6 subnet

**Overview** Use this command to assign an IPv6 subnet to a network entity.  
Use the **no** variant of this command to remove a IPv6 subnet from a network entity.

**Syntax** `ipv6 subnet <ip-network/m> [interface <interface-name>]`  
`no ipv6 subnet <ip-network/m> [interface <interface-name>]`

| Parameter                           | Description  |
|-------------------------------------|--|
| <code>&lt;ip-network/m&gt;</code>   | IPv6 address of the network, entered in the form X:X::X/M, followed by the prefix length in slash notation.  |
| <code>interface</code>              | Specify an interface name. An interface may be specified to add a further restriction on the subnet. No interface configured indicates that any matching address from any interface is a member of this network.         |
| <code>&lt;interface-name&gt;</code> | Interface name. Any AlliedWare Plus interface type (eth, vlan, ppp, tunnel, lo and so on.) followed by any character.<br>A warning message is given if the interface does not match an existing interface on the device. |

**Mode** Network Mode

**Usage notes** You can create multiple subnets for a network entity.

**Examples** To add a subnet to network `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ipv6 subnet 2001:db8::/32
```

To add a subnet and an interface to network `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ipv6 subnet 2001:db8::/32 interface
eth1
```

To add multiple subnets to network servers, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ipv6 subnet 2001:db8::7/32 interface
eth1
awplus(config-network)# ipv6 subnet 2001:db8::8/32 interface
eth1
```

To remove a subnet from network servers, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# no ipv6 subnet 2001:db8::/32
```

**Validation  
commands**    [show entity](#)

**Related  
commands**    [network \(zone\)](#)

# network (zone)

**Overview** Use this command to add a network to a zone entity or configure an existing network.

A network is a high level abstraction of a logical network in a zone. This consists of the IP subnets and interfaces over which it is reachable. Subnets are grouped into networks to apply a common set of rules among the subnets.

Use the **no** variant of this command to destroy a network entity.

**Syntax** `network <network-name>`  
`no network <network-name>`

| Parameter                         | Description   |
|-----------------------------------|---|
| <code>&lt;network-name&gt;</code> | Network name.<br>You can use all alphanumeric ASCII characters, and the dash (-) and underscore (_) characters. The name can be 1 to 64 characters in long. |

**Mode** Zone Mode

**Usage notes** A network is a member of a zone. You can create multiple networks in a zone. A network entity is identified with its parent zone using the dot notation, for example, ZoneName.NetworkName.

This commands allows you to enter the Network Mode with the prompt **awplus(config-network)#**. In the Network Mode, you can:

- Configure subnets and interfaces for the network entity
- Create and delete host entities in the network

A network must have at least one valid network address for it to result in functioning rules using that network entity. For more information about how to add network address, see the [ip subnet](#) command and the [ipv6 subnet](#) command.

Note that if the network entity is destroyed, the subnets and hosts in the network entity will be destroyed as well.

**Example** To create a network entity named `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)#
```

To destroy a network entity named `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# no network servers
```

**Validation  
commands** `show entity`

**Related  
commands** `host (network)`  
`ip subnet`  
`ipv6 subnet`  
`zone`

# protocol

**Overview** Use this command to specify a protocol used by an application.

Protocol numbers are used to configure firewalls, routers, and proxy servers. The protocol number is in the protocol field of the IPv4 header and the next header field of IPv6 header. For the full list of the IP Protocol assignments, you can visit the Internet Assigned Numbers Authority (IANA) website at [www.iana.org](http://www.iana.org).

Use the **no** variant of this command to unset the protocol in an application.

**Syntax** `protocol {tcp|udp|icmp|ipv6-icmp|<protocol-number>}`  
`no protocol`

| Parameter         | Description   |
|-------------------|---|
| tcp               | Transmission Control Protocol. The protocol number is 6.                                      |
| udp               | User Datagram Protocol. The protocol number is 17.  |
| icmp              | Internet Control Message Protocol for Internet Protocol version 4. The protocol number is 1.  |
| ipv6-icmp         | Internet Control Message Protocol for Internet Protocol version 6. The protocol number is 58. |
| <protocol-number> | Protocol number in the range of 0 to 255.   |

**Mode** Application Mode

**Usage notes** You can specify only one protocol for an application. The newly specified protocol will replace the previous one.

**Examples** To specify protocol udp for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# protocol udp
```

To unset the protocol in the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# no protocol
```

**Related commands** [application](#)  
[show application](#)

# show application

**Overview** Use this command to show the custom and predefined applications currently configured.

You can use the [show application detail](#) command to show detailed information of the applications.

**Syntax** `show application`

**Mode** Privileged Exec

**Examples** To show all applications currently configured, use the command:

```
awplus# show application
```

**Output** Figure 29-3: Example output from **show application**

```
awplus#show application
aim          cvs          dns          ftp
http        https       icq          ident
imap        imaps       irc          jabber
l2tp        ldap        lisa        msn
mysql       news        nfs-tcp     nfs-udp
ntp         openvpn     pcanywhere  udp
...
```

**Related commands** [show application detail](#)

# show application detail

**Overview** Use this command to show detailed information about applications that the device is aware of. For custom and predefined applications, the protocol, destination port, source port, ICMP code, ICMP type, DSCP and the name of the applications will be displayed.

**Syntax** `show application detail [<name>|custom]`

| Parameter | Description                         |
|-----------|-------------------------------------|
| <name>    | The name of a specific application. |
| custom    | User-defined application.           |

**Mode** Privileged Exec

**Examples** To show the information about all applications, use the command:

```
awplus# show application detail
```

**Output** To show the information about the application ping, use the command:

```
awplus# show application detail ping
```

Figure 29-4: Example output from **show application detail** for an application

```
awplus#show application detail ping
Name           Mark      Detail
-----
ping           -         proto=ICMP type=8 code=0
```

Table 29-2: Parameters in the output from **show application detail**

| Parameter | Description  |
|-----------|--|
| Name      | Application name—the short name used when referenced from application-aware features (for instance firewall).  |
| Detail    | For custom and pre-defined applications—the IP protocol and port numbers associated with the application. For DPI applications— a longer description of the application. |

**Related commands** [show application](#)

**Command changes** Version 5.4.7-2.1: More detail added to the output for DPI commands.  
Version 5.4.9-1.1: Category added to output for built-in provider

# show entity

**Overview** Use this command to show entity information.

Entity is a high level abstraction of a network device, a group of networks or subnets. It is the instance that firewall policy can be applied to. There are three types of entity:

- zone
- network
- host

**Syntax** `show entity [<entity>]`

| Parameter | Description                      |
|-----------|----------------------------------|
| <entity>  | Specific entity in dot notation. |

**Mode** Privileged Exec

**Examples** To show the information about all entities, use the command:

```
awplus# show entity
```

**Output** Figure 29-5: Example output from the **show entity** command

```
awplus#show entity
Zone:      zone1
Network:   zone1.network1
Subnet:    1:db8:24:100::/64
Subnet:    2001:db8:24:100::/64
Host:      zone1.network1.host1
Address:   2001:db8:24:100::1

Zone:      zone2
Network:   zone2.network2
Host:      zone2.network2.host1
```

To show information associated with the network entity `zone1.network1`, use the command:

```
awplus# show entity zone1.network1
```



**Output** Figure 29-6: Example output from the **show entity** command

```
awplus#show entity zone1.network1
Network:    zone1.network1
Subnet:     1:db8:24:100::/64
Subnet:     2001:db8:24:100::/64
Host:       zone1.network1.host1
Address:    2001:db8:24:100::1
```

To show information associated with the host entity `zone1.network1.host1`, use the command:

```
awplus# show entity zone1.network1.host1
```

**Output** Figure 29-7: Example output from the **show entity** command

```
awplus#show entity zone1.network1.host1
Host:       zone1.network1.host1
Address:    192.168.1.5
```

When the entity is using dynamic interface addresses, this will be shown in the output:

**Output** Figure 29-8: Example output from the **show entity** command

```
awplus#show entity Public
Zone:       Public
Network:    Public.Router
Subnet:     0.0.0.0/0 via ppp0
Host:       Public.Router.ppp0
Address:    10.0.6.1 (dynamic)
```

When the entity is using dynamic FQDN addresses, this will be shown in the output:

**Output** Figure 29-9: Example output from the **show entity** command using dynamic FQDN addresses on the console

```
awplus#show entity Public
Zone:       Public
Network:    Public.FQDNs
Subnet:     0.0.0.0/0
Subnet:     ::/0
Host:       Public.FQDNs.alliedtelesis
FQDN IPv4: alliedtelesis.com
FQDN IPv6: alliedtelesis.com
Address:    54.66.120.42 (dynamic)
```

```
Host:      Public.FQDNs.facebook
FQDN IPv4: facebook.com
FQDN IPv6: facebook.com
Address:   157.240.8.35 (dynamic)
Address:   2a03:2880:f119:8083:face:b00c:0:25de (dynamic)
Host:      Public.FQDNs.google
FQDN IPv4: google.com
FQDN IPv6: google.com
Address:   216.58.196.142 (dynamic)
Address:   2404:6800:4006:809::200e (dynamic)
Host:      Public.FQDNs.microsoft
FQDN IPv4: microsoft.com
FQDN IPv6: microsoft.com
Address:   23.96.52.53 (dynamic)
Address:   23.100.122.175 (dynamic)
Address:   104.40.211.35 (dynamic)
Address:   104.43.195.251 (dynamic)
Address:   191.239.213.197 (dynamic)
```

**Command changes** Version 5.4.8-1.1: added output for dynamic interface and FQDN addresses.

# sport

**Overview** Use this command to specify a source port or a port range used for an application.

A port number is part of the addressing information used to identify a specific process to which a network message is to be forwarded between a sender and a receiver. For the full list of port numbers and their assignment, you can visit the Internet Assigned Numbers Authority (IANA) Web site: [www.iana.org](http://www.iana.org).

Use the **no** variant of this command to delete ports or port ranges from an application.

**NOTE:**

The port or port range that you want to delete must match exactly the existing port or port range. You cannot remove a port range that is part of an existing port range.

**Syntax** `sport {<source-port>|any|<start-range> to <end-range>}`  
`no sport {<source-port>|any|<start-range> to <end-range>}`

| Parameter   | Description   |
|---|---|
| <code>&lt;source-port&gt;</code>                  | The source port number, either TCP or UDP, specified as an integer between 1 and 65535.           |
| <code>any</code>                                  | Any port number in the range <code>&lt;1-65535&gt;</code> . This equals to a range of 1 to 65535. |
| <code>&lt;start-range&gt;</code>                  | Starting port number in the range <code>&lt;1-65535&gt;</code> .                                  |
| <code>to</code><br><code>&lt;end-range&gt;</code> | Ending port number in the range <code>&lt;1-65535&gt;</code> or max.                              |

**Mode** Application Mode

**Usage notes** You can create more than one source port number or port range for an application.

**Examples** To specify source port 500 for the application named `isakmp`, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# sport 500
```

To specify source port 500 and a range of ports for the application named `isakmp`, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# sport 500
awplus(config-application)# sport 60000 to max
```

To specify the source port **any** (a port number range of 1-65535) for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# sport any
```

To remove source port 500 from the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# no sport 500
```

To remove all source ports from the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# no sport 1 to 65535
```

**Related  
commands**

[application](#)  
[dport](#)  
[show application](#)

# zone

**Overview** Use this command to create a zone entity or configure an existing zone.

Zone is a high level abstraction for a logical grouping or segmentation of physical networks. This is the highest level of partitioning that firewall policy can be applied to. Zone establishes the security border of your networks. A zone defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your networks. The minimum zones normally implemented would be a trusted zone for the private network behind the firewall and a untrusted zone for the Internet. Other common zones are a Demilitarized Zone (DMZ) for publicly visible web servers and a Virtual Private Network (VPN) zone for remote access users or tunnels to other networks.

Use the **no** variant of this command to destroy a zone entity.

**Syntax** `zone <zone-name>`  
`no zone <zone-name>`

| Parameter                      | Description   |
|--------------------------------|---|
| <code>&lt;zone-name&gt;</code> | Zone name.<br>You can use all alphanumeric ASCII characters, and the dash (-) and underscore (_) characters. The name can be 1 to 64 characters long. |

**Mode** Global Configuration

**Usage notes** This command allows you to enter the Zone Mode with the prompt **awplus(config-category)#**. The Zone Mode enables you to create, configure and delete network entities. For more information about network entity, see the [network \(zone\)](#) command.

A zone entity must have at least one network entity for it to result in functioning rules using that zone entity. For more information about how to add network entities, see the [network \(zone\)](#) command.

Note that if the zone entity is destroyed, the networks and hosts of this zone will be destroyed as well.

**Examples** To create a zone named `private`, use the commands:

```
awplus# configure terminal
awplus(config)# zone private
awplus(config-zone)#
```

To destroy zone `private` and all its networks, subnets and hosts, use the commands:

```
awplus# configure terminal
awplus(config)# no zone private
```

**Validation** show entity  
**commands**

# 30

# NAT Commands

## Introduction

This chapter provides an alphabetical reference of commands used to configure Network Address Translation (NAT). For more information about NAT introduction and configuration example, see the [Firewall\\_and Network Address Translation \(NAT\) Feature Overview and Configuration\\_Guide](#).

The following figure lists the NAT commands and their applicable modes.

Figure 30-1: NAT commands and applicable modes

| Mode                 | Command                                 |
|----------------------|---|
| Privileged Exec      | <code>show nat</code>                   |
|                      | <code>show nat rule</code>              |
|                      | <code>show nat rule config-check</code> |
|                      | <code>show running-config nat</code>    |
| Global Configuration | <code>nat</code>                        |
| NAT Configuration    | <code>enable (nat)</code>               |
|                      | <code>move rule (nat)</code>            |
|                      | <code>rule (nat)</code>                 |

- Command List**
- [“enable \(nat\)”](#) on page 1273
  - [“ip limited-local-proxy-arp”](#) on page 1274
  - [“local-proxy-arp”](#) on page 1276
  - [“move rule \(nat\)”](#) on page 1277
  - [“nat”](#) on page 1278
  - [“rule \(nat\)”](#) on page 1279

- [“show nat”](#) on page 1283
- [“show nat rule”](#) on page 1284
- [“show nat rule config-check”](#) on page 1286
- [“show running-config nat”](#) on page 1287



# enable (nat)

**Overview** Use this command to enable NAT .

Use the **no** variant of this command to disable NAT without losing existing NAT configuration.

**Syntax** enable  
no enable

**Default** NAT is disabled by default.

**Mode** NAT Configuration

**Examples** To enable NAT, use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# enable
```

To disable NAT, use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# no enable
```

**Validation commands** show nat  
show running-config nat

# ip limited-local-proxy-arp

**Overview** Use this command to enable local proxy ARP, but only for a specified set of IP addresses. This makes the device respond to ARP requests for those IP addresses when the addresses are reachable via the interface you are configuring.

To specify the IP addresses, use the command [local-proxy-arp](#).

Use the **no** variant of this command to disable limited local proxy ARP. This stops your device from intercepting and responding to ARP requests for the specified hosts. This allows the hosts to use MAC address resolution to communicate directly with one another.

**Syntax** `ip limited-local-proxy-arp`  
`no ip limited-local-proxy-arp`

**Default** Limited local proxy ARP is disabled by default.

**Mode** Interface Configuration

**Usage** Limited local proxy ARP supports Static NAT configurations in which the NAT configuration's public address is different to the ethernet interface's address.

On such ethernet interfaces, the device needs to respond to ARP requests for the public address so that it will receive packets targeted at that address.

Limited local proxy ARP makes this possible. It is especially useful when you have a number of 1-1 NAT configurations and each public address falls within the public interface's subnet. If you enable limited local proxy ARP on the public interface and specify suitable addresses, the device will respond to ARP requests for those addresses, as long as the addresses are routed out the interface the ARP requests are received on. The device responds with its own MAC address.

**Example** The following configuration snippet shows how to use limited local proxy ARP, if you are using NAT for an HTTP server with an address of 172.22.0.3 connected via eth1, and eth1 has an address of 172.22.0.1:

```
! Create a private zone for the HTTP server with address 172.22.200.3:
zone private
network vlan1
ip subnet 172.22.200.0/24
host http_server
ip address 172.22.200.3
!
! Create a public zone for the HTTP server with address 172.22.0.3:
zone public
network eth1
ip subnet 0.0.0.0/0 interface eth1
host http_server
ip address 172.22.0.3
!
! Create a NAT rule to map from the public to the private zone:
nat
rule 10 portfwd http from public.eth1 to public.eth1.http_server with dst
private.vlan1.http_server
enable
!
! Configure eth1. It has a different public address than the HTTP server:
interface eth1
ip limited local-proxy-arp
ip address 172.22.0.1/24
!
! Configure vlan1:
interface vlan1
ip address 172.22.200.5/24
!
! Tell the device to respond to ARPs for the HTTP server public address:
local-proxy-arp 172.22.0.3/32
```

**Related commands** [ip local-proxy-arp](#)  
[local-proxy-arp](#)

# local-proxy-arp

**Overview** Use this command to specify an IP subnet for use with limited local proxy ARP. When limited local proxy ARP is enabled with the command [ip limited-local-proxy-arp](#), the device will respond to ARP requests for addresses in that subnet.

Use the **no** variant of this command to stop specifying a subnet for use with limited local proxy ARP.

**Syntax** `local-proxy-arp [<ip-add/mask>]`  
`no local-proxy-arp [<ip-add/mask>]`

| Parameter                        | Description   |
|----------------------------------|---|
| <code>&lt;ip-add/mask&gt;</code> | The IP subnet to use with limited local proxy ARP, in dotted decimal format (A.B.C.D/M). To specify a single IP address, use a 32-bit mask. |

**Default** No subnets are specified for use with limited local proxy ARP.

**Mode** Global Configuration

**Example** To specify limited local proxy ARP for the address 172.22.0.3, use the following commands:

```
awplus# configure terminal
awplus(config)# local-proxy-arp 172.22.0.3/32
```

This is part of a configuration snippet that shows how to use limited local proxy ARP with static NAT. See the command [ip limited-local-proxy-arp](#) for the whole example.

**Related commands** [ip limited-local-proxy-arp](#)

# move rule (nat)

**Overview** Use this command to change the order of a NAT rule.

You can move an existing rule ID only to an ID that is not assigned to any rule, otherwise you will receive an error message.

**Syntax** `move rule <1-65535> to <1-65535>`

| Parameter                              | Description   |
|--|---|
| <code>move rule &lt;1-65535&gt;</code> | Move the order of a given rule. The rule ID of the given rule must exist.<br>Each rule has an ID which is either designated by the user or automatically generated when the rule is created. The rule ID is an integer from 1 to 65535. |
| <code>to &lt;1-65535&gt;</code>        | New rule ID to assign. The new rule ID must not be used by any existing rule.   |

**Mode** NAT Configuration

**Examples** To change the ID of a rule from 10 to 30, use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# move rule 10 to 30
```

**Validation commands** `show nat rule`  
`show running-config nat`

**Related commands** `rule (nat)`

# nat

**Overview** Use this command to configure NAT.

Use the **no** variant of this command to remove all NAT configuration.

**Syntax** nat  
no nat

**Mode** Global Configuration

**Usage notes** This command allows you to enter the NAT Configuration mode. The command prompt for this mode is **awplus(config-nat)#**.

In the NAT Configuration mode, you can:

- Enable NAT, see the [enable \(nat\)](#) command.
- Create NAT rules or change the order of NAT rules, see the [rule \(nat\)](#) command and the [move rule \(nat\)](#) command.

**Examples** To configure NAT, use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)#
```

To remove all NAT configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no nat
```

**Validation commands** [show nat](#)

# rule (nat)

**Overview** Use this command to create a NAT rule.

Use the **no** variant of this command to remove a specified rule or all rules.

**Syntax**

```
rule [<1-65535>] masq <application-name> from <source-entity>  
to <destination-entity> [with src <source-host-entity>]  
  
rule [<1-65535>] portfw <application-name> from <source-entity>  
[to <destination-entity>] with dst <destination-host-entity>  
[dport <1-65535>]  
  
rule [<1-65535>] netmap <application-name> from  
<source-subnet-entity> to <destination-subnet-entity> with  
{src|dst} <translated-subnet-entity>  
  
no rule {<1-65535>|all}
```

| Parameter          | Description   |
|--------------------|---|
| <1-65535>          | Rule ID is an integer in the range 1 to 65535. If you do not designate a rule ID, a rule ID will be automatically generated and it will be greater than the current highest rule ID.  |
| masq               | The type of NAT rule. NAT with IP Masquerade is a case where all or a range of addresses are mapped to a single address with source port translation to identify the association. This single address masquerades as the public source address for the private addresses. |
| portfw             | The type of NAT rule. Port forwarding allows remote hosts to connect to a specific host or service within a private LAN. This will forward IPv4 packets on to another device, for example, forward HTTP traffic to an internal web server.                                |
| netmap             | The type of NAT rule. Use subnet-based NAT to translate the subnet portion of IP addresses while leaving the host portion unchanged.  |
| <application-name> | In all NAT rules, the application name, either one of the predefined applications or an application defined by using the <b>application</b> command.  |

| Parameter                                      | Description   |
|--|---|
| <code>&lt;source-entity&gt;</code>             | Source entity name. An entity represents a logical grouping of subnets, hosts or interfaces, created by the <b>zone</b> , <b>network (Entity)</b> , or <b>host (Entity)</b> commands. In a <b>masq</b> rule, the source entity defines the private side of the router. You assign private IP addresses (RFC 1918) to hosts on the private side of the router. When those hosts send traffic, the router translates the private addresses to one or more publicly valid addresses before routing the traffic. When the router receives traffic that is destined for those hosts, it translates the public addresses back to the appropriate private addresses. In a <b>portfw</b> rule, the source entity may be an entity outside your private network. |
| <code>&lt;destination-entity&gt;</code>        | The destination entity name. The destination entity defines the pool of public-valid IP addresses. It can be a zone (created by the <b>zone</b> command), network ( <b>network (Entity)</b> command) or host ( <b>host (Entity)</b> command).   |
| <code>&lt;source-host-entity&gt;</code>        | In a <b>masq</b> rule, the specific source host address that the traffic will masquerade as. The source -host-entity must be a host with one IP address, created by using the <b>host (Entity)</b> command.   |
| <code>&lt;destination-host-entity&gt;</code>   | In a <b>portfw</b> rule, the target entity name of the specific destination host that the traffic will be port-forwarded to. The target entity must be a host with one IP address, created by using the <b>host (Entity)</b> command.   |
| <code>dport &lt;1-65535&gt;</code>             | In a <b>portfw</b> rule, modify the destination port to the specified port. (Only for protocols that have ports.)   |
| <code>&lt;source-subnet-entity&gt;</code>      | The source entity that the netmap rule will apply to, for instance a network created by the <b>network (Entity)</b> command. When the <b>with src</b> parameter is used, this source-subnet-entity is translated to the <code>&lt;translated-subnet-entity&gt;</code> specified.  |
| <code>&lt;destination-subnet-entity&gt;</code> | The destination entity that the <b>netmap</b> rule applies to, for instance a network created by the <b>network (Entity)</b> command. When the <b>with dst</b> parameter is used, this destination subnet is translated to the <code>&lt;translated-subnet-entity&gt;</code> specified.   |



| Parameter                                     | Description   |
|---|---|
| <code>&lt;translated-subnet-entity&gt;</code> | In a <b>netmap</b> rule:<br><b>with src:</b> Modify the source-subnet-entity to the specified translated-subnet-entity, for instance a network created by the <b>network (Entity)</b> command. Both network entities must contain one subnet with a matching subnet mask.<br><b>with dst:</b> Modify the destination-subnet-entity to the specified translated-subnet-entity, for instance a network created by the <b>network (Entity)</b> command. Both network entities must contain one subnet with a matching subnet mask. |
| all   | Remove all rules.   |

**Mode** NAT Configuration

**Usage notes** You can change the rule order by using the [move rule \(nat\)](#) command.

Firewall is used in conjunction with NAT. Port forwarding (**portfw**) and masquerade (**masq**) rules do not implicitly permit packets. **Portfw** rules (actions) are applied before any other firewall and **masq** rules (actions) are applied after any other firewall rules. When firewall protection is enabled, all traffic is blocked by default. Use the [rule \(firewall\)](#) command to configure firewall rules which allow the same application, source and destination entities you configure for the NAT rules.

Netmap **dst** rules are applied to traffic before it reaches the firewall rules, and netmap **src** rules are applied after the firewall has permitted the traffic. Firewall rules must be written to permit the traffic after it has been translated by the netmap **dst** rules.

Entities should have valid interfaces on which inbound and outbound traffic can be properly translated. You can use the [ip subnet](#) command and the [ipv6 subnet](#) command to configure the interfaces.

Removing a NAT rule for an actively translated flow does not stop it translating immediately. This means subsequent packets in the flow continue to be translated.

The continued translation after the associated NAT rule is removed will only stop when:

- The [clear firewall connections](#) command is executed or the flow stops.
- One of the following actions occurs:
  - You can use the [clear firewall connections](#) command to manually stop translations immediately, when the associated rule has been deleted regardless whether the firewall feature is actually configured with NAT or not.
  - The NAT rule is cleared when the traffic flow ends naturally, for example, stopped from the source. If the flow is re-initiated from a host, it will not be translated by the firewall, as the rule is deleted after the first flow stopped.

**Examples** To perform network address translation and port forward application 'http' from entity 'public' to any with target destination dmz.servers.web\_server, use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# rule 10 portfw
http from public with dst dmz.servers.web_server
```

To perform network address translation and masquerade application 'http' from entity 'private' to 'public', use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# rule 20 masq
http from private to public
```

To use subnet-based NAT to translate the source address of all traffic from 'private.lan' going to 'remote.lan' with the new subnet specified in 'private.global', use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# rule 30 netmap all from private.lan to
remote.lan with src private.global
```

To remove NAT rule 10, use the command:

```
awplus(config-nat)# no rule 10
```

**Related  
commands**

[application](#)  
[clear firewall connections](#)  
[host \(network\)](#)  
[move rule \(nat\)](#)  
[nat](#)  
[network \(zone\)](#)  
[show nat rule](#)  
[show nat rule config-check](#)  
[show running-config nat](#)  
[zone](#)

**Command  
changes** Version 5.4.7-0.1: **netmap** option added.

# show nat

**Overview** Use this command to show the configuration state of NAT.

**Syntax** show nat

**Mode** Privileged Exec

**Examples** To show the configuration state of NAT, use the commands:

```
awplus# show nat
```

**Output** Figure 30-2: Example output from the **show nat** command

```
awplus#show nat
NAT is enabled
```

**Related commands** [enable \(nat\)](#)

# show nat rule

**Overview** Use this command to show information about NAT rules.

**Syntax** show nat rule [<1-65535>]

| Parameter | Description |
|-----------|-------------|
| <1-65535> | Rule ID     |

**Mode** Privileged Exec

**Examples** To show information about all NAT rules, use the command:

```
awplus# show nat rule
```

**Output** Figure 30-3: Example output from the **show nat rule** command

```
awplus#show nat rule

[* = Rule is not valid - see "show nat rule config-check"]
  ID      Action  App      From      To      With      Hits
-----
* 30     masq    any      private   public   -         0
  10     portfw  http     public    -        dmz.a.b   0
```

To show information about a specific NAT rule, use the command:

```
awplus# show nat rule 10
```

**Output** Figure 30-4: Example output from the **show nat rule** command

```
awplus#show nat rule 10

[* = Rule is not valid - see "show nat rule config-check"]
  ID      Action  App      From      To      With      Hits
-----
  10     portfw  http     public    -        dmz.a.b   0
```

| Output Parameter | Description  |
|------------------|--|
| *                | Indicates the rule is not valid and cannot be hit, see the <a href="#">show nat rule config-check</a> command. |
| App              | Application name.  |
| From             | Source entity.   |

| Output Parameter | Description                                    |
|------------------|--|
| with             | Target entity name.                            |
| To               | Destination entity.                            |
| Hits             | The number of times the NAT rule has been hit. |

**Related commands** [rule \(nat\)](#)  
[show nat rule config-check](#)

# show nat rule config-check

**Overview** Use this command to check configuration validity of NAT rules.

An invalid rule will not be active and cannot be hit.

This command also shows the reasons why a rule is not valid.

**Syntax** `show nat rule config-check`

**Mode** Privileged Exec

**Usage notes** NAT rules are applied to applications and entities. A rule is not valid if either the application, source entity or destination entity the rule applies to is not configured properly.

To configure applications and entities, see Application and Entity Commands.

**Examples** To check configuration validity of NAT rules, use the command:

```
awplus# show nat rule config-check
```

**Output** Figure 30-5: Example output from the **show nat rule config-check** command if rule configuration errors are detected

```
awplus#show nat rule config-check
Rule 10:
  Application does not have a protocol configured
  "From" entity does not exist
  "To" entity has no subnet or host addresses
```

**Output** Figure 30-6: Example output from the **show nat rule config-check** command if all rules are valid

```
awplus#show nat rule config-check
All rules are valid
```

# show running-config nat

**Overview** Use this command to show the configuration commands that have been used to configure NAT.

**Syntax** `show running-config nat`

**Mode** Privileged Exec

**Examples** To show the configuration commands that have been used to configure NAT, use the commands:

```
awplus# show running-config nat
```

**Output** Figure 30-7: Example output from the **show running-config nat** command

```
awplus#show running-config nat
nat
 rule 10 masq http from private to public
 rule 20 portfw http from public with dst dmz.servers.wb
 enable
!
```

# Part 7: Advanced Network Protection



# 31

# IPS Commands

## Introduction

This chapter provides an alphabetical reference of commands used to configure Intrusion Prevention System (IPS). For more information, see the [IPS Feature Overview and Configuration\\_Guide](#).

The table below lists the IPS commands and their applicable modes.

Figure 31-1: IPS Commands and Applicable Modes

| Mode                 | Command                              |
|----------------------|--------------------------------------|
| Privileged Exec      | <code>show ips</code>                |
|                      | <code>show ips categories</code>     |
|                      | <code>show running-config ips</code> |
| Global Configuration | <code>ips</code>                     |
| IPS Mode             | <code>category action (IPS)</code>   |
|                      | <code>protect (IPS)</code>           |

- Command List**
- [“category action \(IPS\)”](#) on page 1290
  - [“ips”](#) on page 1291
  - [“protect \(IPS\)”](#) on page 1292
  - [“show ips”](#) on page 1293
  - [“show ips categories”](#) on page 1294
  - [“show running-config ips”](#) on page 1296

# category action (IPS)

**Overview** Use this command to configure an action for a specified category.  
Use the **no** variant of this command to set the default action of alert for a specified category.

**Syntax** `category <category-name> action {alert|deny|disable}`  
`no category <category-name> action`

| Parameter                          | Description  |
|------------------------------------|--|
| <code>&lt;category-name&gt;</code> | Category name. A category is a label that helps to classify the nature of traffic, for example, whether it is spammer, spot or spyware and so on. Once IPS protection is enabled, traffic will be categorized according to the available IPS categories. You can use the <a href="#">show ips categories</a> command to view the categories and their actions. |
| <code>alert</code>                 | Generate a log message. This is the default action.  |
| <code>deny</code>                  | Drop the matching packets. No error message is sent back to the source host.   |
| <code>disable</code>               | Ignore a specified category. Ignored categories will not be used to categorize traffic.  |

**Default** The default action is alert.

**Mode** IPS Mode

**Examples** To drop packet categorized as checksum, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# category checksum action deny
```

To set the default action for category checksum, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no category checksum action
```

**Validation Commands** [show ips categories](#)  
[show running-config ips](#)

# ips

**Overview** Use this command to configure IPS.

Use the **no** variant of this command to remove all IPS configuration.

**Syntax** `ips`  
`no ips`

**Mode** Global Configuration

**Usage notes** This command allows you to enter the IPS mode. The command prompt for this mode is **awplus(config-ips)#**.

In the IPS mode, you can:

- Enable or disable IPS protection, see the [protect \(IPS\)](#) command.
- Configure an action for specified categories, see the [category action \(IPS\)](#) command.

**Examples** To configure IPS, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)#
```

To remove all IPS configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no ips
```

# protect (IPS)

**Overview** Use this command to enable IPS protection .  
Use the **no** variant of this command to disable IPS protection.

**Syntax** protect  
no protect

**Usage notes** Once IPS protection is enabled, traffic will be categorized according to the available IPS categories. See the [show ips categories](#) command for the list of available IPS categories.

**Default** IPS is disabled by default.

**Mode** IPS Mode

**Examples** To enable IPS protection, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# protect
```

To disable IPS protection, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no protect
```

**Validation Commands** [show ips](#)  
[show running-config ips](#)

# show ips

**Overview** Use this command to show the IPS configuration state and event count for the Intrusion Prevention System (IPS).

**Syntax** `show ips`

**Mode** Privileged Exec

**Examples** To display information about IPS, use the command:

```
awplus# show ips
```

**Output** Figure 31-2: Example output from the **show ips** command

```
awplus#show ips
Status:      Enabled (Active)
Events:      4
```

**Command changes** Version 5.4.7-0.1: Event count added to the command output.

# show ips categories

**Overview** Use this command to show the IPS categories and their actions.

Note that if the IPS database provider is configured, this commands shows only the provider's categories.

**Syntax** `show ips categories`

**Mode** Privileged Exec

**Examples** To show the IPS categories and their actions, use the command:

```
awplus# show ips categories
```

**Output** Figure 31-3: Example output of built-in categories from the **show ips categories** command

```
awplus#show ips categories
Category (* = invalid)      Action
-----
checksum                    alert
ftp-bounce                  alert
gre-decoder-events         alert
http-events                 alert
icmp-decoder-events        alert
ip-decoder-events          alert
ppp-decoder-events         alert
smtp-events                alert
stream-events              alert
udp-decoder-events         alert
```

| Parameter          | Description  |
|--------------------|--|
| checksum           | Invalid checksums, e.g. IPv4, TCPv4, UDPv4, ICMPv4, TCPv6, UDPv6, ICMPv6.  |
| ftp-bounce         | GPL FTP PORT bounce attempt.   |
| gre-decoder-events | GRE anomalies, e.g. GRE packet too small, GRE wrong version, GRE v0 recursion control, GRE v0 flags, GRE v0 header too big, GRE v1 checksum present, GRE v1 routing present, GRE v1 strict source route, GRE v1 recursion control.   |
| http-events        | HTTP anomalies, e.g. HTTP unknown error, HTTP gzip decompression failed, HTTP request field missing colon, HTTP response field missing colon, HTTP invalid request chunk len, HTTP invalid response chunk len, HTTP status 100-Continue already seen, HTTP unable to match response to request, HTTP invalid server port in request. |

| Parameter           | Description  |
|---------------------|--|
| icmp-decoder-events | ICMP anomalies, e.g. IPv6 with ICMPv4 header, ICMPv4 packet too small, ICMPv4 unknown type, ICMPv6 truncated packet, ICMPv6 unknown version.   |
| ip-decoder-events   | IPv4 & IPv6 anomalies, e.g. IPv4 packet too small, IPv4 header size too small, IPv4 wrong IP version, IPv6 packet too small, IPv6 duplicated Routing extension header, IPv6 duplicated Hop-By-Hop Options extension header, IPv6 DSTOPTS only padding, SLL packet too small, Ethernet packet too small, VLAN header too small, FRAG IPv4 Fragmentation overlap, FRAG IPv6 Packet size too large, IPv4-in-IPv6 invalid protocol, IPv6-in-IPv6 packet too short. |
| ppp-decoder-events  | PPP anomalies, e.g. PPP packet too small, PPP IPv6 too small, PPP wrong type, PPPoE wrong code, PPPoE malformed tags.  |
| smtp-events         | SMTP anomalies, e.g. SMTP invalid reply, SMTP max reply line len exceeded, SMTP tls rejected, SMTP data command rejected.  |
| stream-events       | TCP anomalies, e.g. 3way handshake with ack in wrong dir, 3way handshake async wrong sequence, 3way handshake right seq wrong ack evasion, 4way handshake SYNACK with wrong ACK, STREAM CLOSEWAIT FIN out of window, STREAM ESTABLISHED SYNACK resend, STREAM FIN invalid ack, STREAM FIN1 ack with wrong seq, STREAM TIMEWAIT ACK with wrong seq, stream-events TCP packet too small, stream-events TCP duplicated option)                                    |
| udp-decoder-events  | UDP anomalies, e.g. UDP packet too small, UDP header length too small, UDP invalid header length   |

# show running-config ips

**Overview** Use this command to show the configuration commands that have been used to configure IPS.

**Syntax** `show running-config dpi`

**Mode** Privileged Exec

**Examples** To show the commands that have been used to configure IPS, use the command:

```
awplus# show running-config ips
```

**Output** Figure 31-4: Example output from the **show running-config ips** command

```
awplus#show running-config ips
ips
 protect
!
```



# 32

# URL Filtering Commands

## Introduction

This chapter provides an alphabetical reference of commands used to configure URL filtering.

URL filtering blocks all HTTP and HTTPS access to a list of websites. You can specify a short list of websites (up to 1000 blacklist and 1000 whitelist rules) using custom blacklists to block URLs and custom whitelists to allow access to URLs.

For more information, see the [URL Filtering Feature Overview\\_and Configuration Guide](#).

The following table lists the URL filtering commands and their applicable modes.

Figure 32-1: URL filtering commands and applicable modes

| Mode                     | Command                                     |
|--------------------------|---|
| Privileged Exec          | <code>show running-config url-filter</code> |
|                          | <code>show url-filter</code>                |
|                          | <code>url-filter reload custom-lists</code> |
| Global Configuration     | <code>url-filter</code>                     |
| URL Filter Configuration | <code>blacklist</code>                      |
|                          | <code>protect (url-filter)</code>           |
|                          | <code>whitelist (url-filter)</code>         |

- Command List**
- `"blacklist"` on page 1299
  - `"log url-requests"` on page 1300
  - `"protect (url-filter)"` on page 1301
  - `"show running-config url-filter"` on page 1302
  - `"show url-filter"` on page 1303

- [“url-filter reload custom-lists”](#) on page 1304
- [“url-filter”](#) on page 1305
- [“whitelist \(url-filter\)”](#) on page 1306

# blacklist

**Overview** Use this command to add a custom blacklist file to the URL filtering configuration. Use the **no** variant of this command to remove a blacklist from the URL filtering configuration.

**Syntax** `blacklist <location_of_blacklist_file>`  
`no blacklist <location_of_blacklist_file>`

| Parameter                                       | Description  |
|---|--|
| <code>&lt;location_of_blacklist_file&gt;</code> | Location of the blacklist file. The blacklist file can be located in flash or on a USB device. |

**Mode** URL Filter Configuration

**Usage notes** You can use custom blacklists to specify URLs to be blocked.

For information about blacklist rule format, see the [URL Filtering Feature Overview and Configuration Guide](#).

You can use the [whitelist \(url-filter\)](#) command to add a whitelist that will override any corresponding blacklist entries.

**Examples** To add a blacklist that uses a custom file that is stored on a USB device, and then enable URL filtering, use the commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# blacklist usb:/my_blacklist.txt
awplus(config-url-filter)# protect
```

To remove that blacklist file from the URL filtering configuration, use the commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# no blacklist usb:/my_blacklist.txt
```

**Related commands**

- [protect \(url-filter\)](#)
- [show url-filter](#)
- [url-filter reload custom-lists](#)
- [whitelist \(url-filter\)](#)

# log url-requests

**Overview** If URL Filtering is enabled, then by default, black list hits and issues with match criteria and list files are logged.

Use this command to enable logging of all HTTP and HTTPS URL requests (both permitted and denied) passing through the firewall.

Use the **no** variant of this command to disable extra logging of HTTP and HTTPS URL requests passing through the firewall.

**Syntax** `log url-requests`  
`no log url-requests`

**Default** Disabled by default.

**Mode** URL Filter Configuration

**Usage notes** When enabled, additional log messages for HTTP and HTTPS URL requests passing through the firewall contain the:

- URL being accessed
- IP address of the user that requested the URL

**Example** To configure logging of all HTTP and HTTPS URL requests passing through the firewall (permitted as well as denied), use the following commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# log url-requests
```

**Related commands** [url-filter](#)

**Command changes** Version 5.4.7-1.1: command added

# protect (url-filter)

- Overview** Use this command to enable URL filter protection.
- Use the **no** variant of this command to disable URL filter protection without losing the existing URL filter configuration.
- Syntax** `protect`  
`no protect`
- Default** URL filter protection is disabled by default and all HTTP and HTTPS traffic is allowed.
- Mode** URL Filter Configuration
- Examples** To enable URL filter protection, use the commands:
- ```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# protect
```
- To disable URL filter protection, use the commands:
- ```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# no protect
```
- Related commands** [show url-filter](#)
- Command changes** Version 5.4.7-1.1: HTTPS support added.

# show running-config url-filter

**Overview** Use this command to show the running configuration information for URL filtering

**Syntax** `show running-config url-filter`

**Mode** Privileged Exec

**Examples** To show the running configuration of URL filtering, use the command:

```
awplus# show running-config url-filter
```

# show url-filter

**Overview** Use this command to show information about the configuration state of URL filtering.

**Syntax** `show url-filter`

**Mode** Privileged Exec

**Examples** To show information about the configuration state of URL filtering, use the command:

```
awplus# show url-filter
```

**Output** Figure 32-2: Example output from **show url-filter**

```
awplus#show url-filter
Status:      Enabled (Active)
Events:      104
Custom blacklists  Entries
blacklist-example.txt  365
Custom whitelists  Entries
whitelist-example.txt  4
```

**Command changes** Version 5.4.7-0.1: Event count added to the command output.

# url-filter reload custom-lists

**Overview** Use this command to reload all custom blacklists and whitelists after editing one or more of them.

**Syntax** `url-filter reload custom-lists`

**Mode** Privileged Exec

**Examples** To reload all custom blacklists and whitelists, use the following command:

```
awplus# url-filter reload custom-lists
```

**Related commands** [blacklist](#)  
[whitelist \(url-filter\)](#)



# url-filter

**Overview** Use this command to enter URL Filter Configuration mode and configure URL filtering functionality.

Use the **no** variant of this command to remove all URL filtering configuration.

**Syntax** url-filter  
no url-filter

**Mode** Global Configuration

**Usage notes** This command allows you to enter the URL Filter Configuration mode and changes the command prompt to **awplus(config-url-filter)#**.

The URL Filter Configuration mode enables you to:

- Enable URL filtering protection; see the [protect \(url-filter\)](#) command.
- Configure custom blacklists; see the [blacklist](#) command.
- Configure custom whitelists; see the [whitelist \(url-filter\)](#) command.

**Examples** To enter the URL Filter Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)#
```

To remove all URL filter configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no url-filter
```

**Related commands** [blacklist](#)  
[protect \(url-filter\)](#)  
[show running-config](#)  
[show url-filter](#)  
[whitelist \(url-filter\)](#)

# whitelist (url-filter)

**Overview** Use this command to add a custom whitelist file to the URL filtering configuration. Use the **no** variant of this command to remove a whitelist from the URL filter configuration.

**Syntax** `whitelist <url_of_whitelist_file>`  
`no whitelist <location_of_whitelist_file>`

| Parameter                                       | Description  |
|---|--|
| <code>&lt;location_of_whitelist_file&gt;</code> | Location of the whitelist file. The whitelist file can be located in flash or on a USB device. |

**Mode** URL Filter Configuration

**Usage notes** Whitelist matching precedes blacklist matching. You can use custom whitelists to override any corresponding blacklist entries. An HTTP or HTTPS request that includes a URL that matches an entry in a whitelist will be permitted.

For information about whitelist rule format, see the [URL Filtering Feature Overview and Configuration Guide](#).

**Examples** To add a whitelist that uses a custom file that is stored on a USB device, and then enable URL filtering, use the commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# whitelist usb:/my_whitelist.txt
awplus(config-url-filter)# protect
```

To remove that whitelist file from the URL filtering configuration, use the commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# no whitelist usb:/my_whitelist.txt
```

**Related commands** [blacklist](#)  
[protect \(url-filter\)](#)  
[show url-filter](#)  
[url-filter reload custom-lists](#)

**Command changes** Version 5.4.7-1.1: HTTPS support added.

# Part 8: Virtual Private Networks (VPNs)

# 33

# IPsec Commands

## Introduction

This chapter provides an alphabetical reference of commands used to configure Internet Protocol Security (IPsec) tunnel.

For introductory information about IPsec tunnel in AlliedWare Plus, including overview and configuration information, see the:

- [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#)
- [GRE and Multipoint VPNs Feature Overview and Configuration Guide](#)

### Command List

- [“clear isakmp sa”](#) on page 1310
- [“crypto ipsec profile”](#) on page 1311
- [“crypto isakmp key”](#) on page 1313
- [“crypto isakmp peer”](#) on page 1316
- [“crypto isakmp profile”](#) on page 1318
- [“debug isakmp”](#) on page 1320
- [“dpd-interval”](#) on page 1322
- [“dpd-timeout”](#) on page 1323
- [“interface tunnel \(IPsec\)”](#) on page 1324
- [“lifetime \(IPsec Profile\)”](#) on page 1325
- [“lifetime \(ISAKMP Profile\)”](#) on page 1326
- [“no debug isakmp”](#) on page 1327
- [“pfs”](#) on page 1328
- [“rekey”](#) on page 1330
- [“show debugging isakmp”](#) on page 1331
- [“show interface tunnel \(IPsec\)”](#) on page 1332

- [“show ipsec counters”](#) on page 1333
- [“show ipsec peer”](#) on page 1334
- [“show ipsec policy”](#) on page 1335
- [“show ipsec profile”](#) on page 1336
- [“show ipsec sa”](#) on page 1338
- [“show isakmp counters”](#) on page 1339
- [“show isakmp key \(IPsec\)”](#) on page 1340
- [“show isakmp peer”](#) on page 1341
- [“show isakmp profile”](#) on page 1342
- [“show isakmp sa”](#) on page 1344
- [“transform \(IPsec Profile\)”](#) on page 1345
- [“transform \(ISAKMP Profile\)”](#) on page 1346
- [“tunnel destination \(IPsec\)”](#) on page 1348
- [“tunnel local name \(IPsec\)”](#) on page 1350
- [“tunnel local selector”](#) on page 1351
- [“tunnel mode ipsec”](#) on page 1353
- [“tunnel protection ipsec \(IPsec\)”](#) on page 1354
- [“tunnel remote name \(IPsec\)”](#) on page 1355
- [“tunnel remote selector”](#) on page 1356
- [“tunnel security-reprocessing”](#) on page 1358
- [“tunnel selector paired”](#) on page 1359
- [“tunnel source \(IPsec\)”](#) on page 1360
- [“undebg isakmp”](#) on page 1362
- [“version \(ISAKMP\)”](#) on page 1363

# clear isakmp sa

**Overview** Use this command to delete Internet Security Association Key Management Protocol (ISAKMP) Security Associations (SAs). SAs specify the Security Parameter Index (SPI), protocols, algorithms and keys for protecting a single flow of traffic between two IPsec peers. For more information about SA, see the [Internet Protocol Security \(IPSec\) Feature Overview and Configuration Guide](#).

**Syntax** `clear [crypto] isakmp sa [peer <ipv4-addr>|<ipv6-addr>|<hostname>] [force]`

| Parameter   | Description  |
|-------------|--|
| <ipv4-addr> | Destination IPv4 address. The IPv4 address uses the format A.B.C.D.  |
| <ipv6-addr> | Destination IPv6 address. The IPv4 address uses the format X:X::X:X. |
| <hostname>  | Destination host name.   |
| force       | Force to clear ISAKMP SAs without negotiating with the peer.         |

**Mode** Privileged Exec

**Examples** To delete the ISAKMP security associations at the peer for an IPv6 address, use the command:

```
awplus# clear isakmp sa peer 2001:0db8::1
```

To delete the ISAKMP security associations at the peer for an IPv4 address, use the command:

```
awplus# clear isakmp sa peer 192.168.2.1
```

To delete the ISAKMP security associations at the peer for a host name, use the command:

```
awplus# clear isakmp sa peer remote.example.com
```

**Related commands** [crypto isakmp key](#)  
[show isakmp sa](#)

**Command Changes** Version 5.4.7-0.1: Parameter <hostname> added for DDNS feature.

# crypto ipsec profile

**Overview** Use this command to configure a custom IPsec profile.

An IPsec profile comprises one or more transforms that can be configured by using the [transform \(IPsec Profile\)](#) command.

Use the **no** variant to delete a previously created profile.

**Syntax** `crypto ipsec profile <profile_name>`  
`no crypto ipsec profile <profile_name>`

| Parameter                         | Description  |
|-----------------------------------|--|
| <code>&lt;profile_name&gt;</code> | Profile name. Profile names are case insensitive and can be up to 64 characters long composed of printable ASCII characters. Profile names can have only letters from a to z and A to Z, numbers from 0 to 9, - (dash), or _ (underscore). |

**Default** The default IPsec profile with transforms in order of preference is listed in the following table. Which IPsec profile will actually be used depends on how the negotiation between the peers is carried out when establishing the connection. Note that you cannot delete or edit the default profile. Expiry time of 8 hours applies to the default IPsec profile.

Table 33-1: IPsec default profile

| Attribute            | Transform 1 | Transform 2 | Transform 3 | Transform 4 | Transform 5 | Transform 6 |
|----------------------|-------------|-------------|-------------|-------------|-------------|-------------|
| Protocol             | ESP         | ESP         | ESP         | ESP         | ESP         | ESP         |
| Encryption (all CBC) | AES256      | AES256      | AES128      | AES128      | 3DES        | 3DES        |
| Integrity (all HMAC) | SHA256      | SHA1        | SHA256      | SHA1        | SHA256      | SHA1        |

**Mode** Global Configuration

**Examples** To configure a custom IPsec profile for establishing IPsec SAs with a remote peer, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# transform 2 protocol esp
integrity sha1 encryption 3des
```

To delete a custom profile, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto ipsec profile my_profile
```

**Related  
commands**    lifetime (IPsec Profile)  
                  show ipsec profile  
                  transform (IPsec Profile)



# crypto isakmp key

**Overview** Use this command to configure a pre-shared authentication key.

Pre-shared key authentication uses optionally-encrypted shared keys identified by hostname, IPv4 or IPv6 address. Pre-shared keys are not viewable and are stored encrypted in the running-configuration.

You must configure this key whenever you specify pre-shared keys in an (Internet Key Exchange) IKE policy and at both peers.

This command specifies both the value of the pre-shared key and also an identifier (the hostname, address or policy parameters). This identifier is used to decide which pre-shared key to use for a particular ISAKMP message exchange.

See the Usage section below for more information, and see the following guides for examples:

- [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#)
- [GRE and Multipoint VPNs Feature Overview and Configuration Guide](#)

Use the **no** variant to remove a pre-shared key.

**Syntax**

```
crypto isakmp key [8] <key> hostname <hostname> [type {eap|psk}]
no crypto isakmp key [8] <key> hostname <hostname> [type {eap|psk}]

crypto isakmp key [8] <key> address {<ipv4-addr>|<ipv6-addr>}
[type {eap|psk}]

no crypto isakmp key [8] <key> address
{<ipv4-addr>|<ipv6-addr>} [type {eap|psk}]

crypto isakmp key [8] <key> policy <policy-name> [type
{eap|psk}]

no crypto isakmp key [8] <key> policy <policy-name> [type
{eap|psk}]
```

| Parameter   | Description   |
|-------------|---|
| crypto      | Security specific command.  |
| isakmp      | Internet Security Association Key Management Protocol provides a common framework for key management implementations. |
| key         | Pre-shared key.   |
| <key>       | Specify the pre-shared key. Use any combination of alphanumeric characters up to 128 bytes.                           |
| 8           | Specifies that an encrypted key follows.  |
| <hostname>  | A hostname (e.g. example.com).  |
| <ipv4-addr> | IPv4 address. The IPv4 address uses the format A.B.C.D.   |

| Parameter     | Description  |
|---------------|--|
| <ipv6-addr>   | IPv6 address. The IPv6 address uses the format X:X::X:X.   |
| <policy-name> | The local policy name. This is the name of the tunnel (e.g. tunnel2).  |
| type          | ISAKMP key type  |
| eap           | Extensible Authentication Protocol. This can be used with multipoint VPN when performing RADIUS authentication. See the <a href="#">GRE and Multipoint VPNs Feature Overview and Configuration Guide</a> for more information. |
| psk           | Pre-shared Key (default)   |

**Default** ISAKMP keys do not exist.

**Mode** Global Configuration

**Usage notes** Use this command to configure a pre-shared authentication key for use with the ISAKMP protocol.

Before a tunnel can be protected by IPsec, each endpoint of the tunnel must verify that they are communicating with an authorized entity. ISAKMP uses pre-shared keys in the initial handshake between peers to ensure both endpoints are allowed to communicate.

This command specifies both the value of the pre-shared key and also an identifier which is used to decide which pre-shared key to use for a particular ISAKMP message exchange. Because the responding endpoint does not identify itself to the local device until after the pre-shared key is used, it is important that the key identifier is part of the tunnel configuration on the initiating device.

The tunnel configuration parameter used to select which pre-shared key to use when negotiating IPsec protection for that tunnel is in priority order:

- 1) **tunnel remote name**
- 2) **tunnel destination <ipv4-address>|<ipv6-address>** (if the remote name is not specified)
- 3) **tunnel local name**
- 4) **tunnel source <ipv4-address>|<ipv6-address>** (if the remote name is not specified)

For point-to-point tunnels, we recommend you configure local and remote names on the tunnels. Then use the remote name of the other device to identify the pre-shared keys on the local device.

For point-to-multipoint tunnels, it may be necessary to identify the pre-shared key by the local name of the tunnel, if the ISAKMP negotiation is to be initiated by that tunnel. This is because it is not possible to configure multiple remote names. However, it is possible to use the expected remote addresses or names of the remote initiating tunnels to identify keys. This is because the remote tunnel will identify itself when it initiates a connection.

**Examples** To configure a pre-shared authentication key of “friend”, using a hostname, use the commands below:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend hostname
mypeer@my.domain.com
```

To remove that pre-shared key, use the commands below:

```
awplus# configure terminal
awplus(config)# no crypto isakmp key friend hostname
mypeer@my.domain.com
```

To configure a pre-shared already-encrypted authentication key, using an IPv4 address, use the commands below:

```
awplus# configure terminal
awplus(config)# crypto isakmp key 8 Nhe6ioQmzbysQaJr6Du+cA==
address 192.168.1.2
```

To configure a pre-shared key, using the local policy “tunnel2”, use the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend policy tunnel2
```

To remove that key, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp key friend policy tunnel2
```

To configure an ISAKMP key using EAP, enter the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend hostname example.com
type eap
```

**Related commands**

- [show isakmp key \(IPsec\)](#)
- [tunnel destination \(IPsec\)](#)
- [tunnel local name \(IPsec\)](#)
- [tunnel remote name \(IPsec\)](#)

**Command changes**

- Version 5.4.9-0.1: **type** parameter added
- Version 5.4.9-1.1: **policy** parameter added

# crypto isakmp peer

**Overview** Use this command to configure a peer to use a specific ISAKMP profile.

Use the **no** variant to set the peer back to using the default profile.

**Syntax**

```
crypto isakmp peer address {<ipv4-addr>|<ipv6-addr>} profile
<profile-name>
no crypto isakmp peer address {<ipv4-addr>|<ipv6-addr>} profile
crypto isakmp peer dynamic profile <profile-name>
no crypto isakmp peer dynamic profile
crypto isakmp peer hostname <hostname> profile <profile-name>
no crypto isakmp peer hostname <hostname> profile
crypto isakmp peer policy <policy-name> profile <profile-name>
no crypto isakmp peer policy <policy-name> profile
```

| Parameter      | Description  |
|----------------|--|
| <ipv4-addr>    | IPv4 address. The IPv4 address uses the format A.B.C.D.                    |
| <ipv6-addr>    | IPv6 address. The IPv6 address uses the format X:X::X:X.                   |
| dynamic        | Remote endpoint with a dynamic IP address.                                 |
| <hostname>     | Remote endpoint with a host name as the destination.                       |
| <policy-name>  | The name of a local policy. This is the name of the tunnel (e.g. tunnel2). |
| <profile-name> | Profile name.  |

**Default** By default, all peers use the default profile.

**Mode** Global Configuration

**Usage notes** Use this command to configure a peer to use a specific ISAKMP profile.

When IPsec protection is applied to a tunnel, an ISAKMP profile is selected for use when IPsec parameters need to be negotiated. This profile is chosen when the tunnel first becomes active, and so must be selected based on local configuration only.

The tunnel configuration parameter used to select which ISAKMP profile to use when negotiating IPsec protection for that tunnel is in the following priority order:

- 1) **tunnel destination dynamic** (if a dynamic profile has been configured)
- 2) **tunnel endpoint dynamic** (if a dynamic profile has been configured)
- 3) **tunnel remote name**

- 4) **tunnel destination** <ipv4-address>|<ipv6-address> (if the remote name is not specified)
- 5) **tunnel endpoint** <ipv4-address>
- 6) **tunnel local name**
- 7) **tunnel source** <ipv4-address>|<ipv6-address> (if the remote name is not specified)
- 8) **tunnel destination** <hostname> (if the hostname is not specified)
- 9) **tunnel endpoint** <hostname> (if the hostname is not specified)

**Examples** To configure a profile for a peer, using a dynamic IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp peer dynamic profile peer_profile
```

To set the profile for the peer back to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp peer dynamic profile
```

To configure a profile for a peer, using a local policy name of "tunnel2", use the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp peer policy tunnel2 profile
peer-profile
```

To set the profile for the peer back to the default, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp peer policy tunnel2 profile
```

**Related commands**

- [show isakmp peer](#)
- [tunnel destination \(IPsec\)](#)
- [tunnel local name \(IPsec\)](#)
- [tunnel source \(IPsec\)](#)
- [tunnel remote name \(IPsec\)](#)

**Command Changes**

- Version 5.4.7-0.1: **hostname** parameter added.
- Version 5.4.9-1.1: **policy** parameter added.

# crypto isakmp profile

**Overview** Use this command to configure a custom ISAKMP profile.

An ISAKMP profile comprises one or more transforms that can be configured by using the [transform \(ISAKMP Profile\)](#) command.

Use the **no** variant to delete a previously created profile.

**Syntax** `crypto isakmp profile <profile_name>`  
`no crypto isakmp profile <profile_name>`

| Parameter                         | Description  |
|-----------------------------------|--|
| <code>&lt;profile_name&gt;</code> | Profile name. Profile names are case insensitive and can be up to 64 characters long composed of printable ASCII characters. Profile names can have only letters from a to z and A to Z, numbers from 0 to 9, - (dash), or _ (underscore). |

**Default** Which ISAKMP profile transform will actually be used depends on how the negotiation between the peers is carried out when establishing the connection. For more information about default ISAKMP profiles, see the following table. Note that you cannot delete or edit the default profile. Expiry time of 24 hours applies to the default profile.

Table 33-2: ISAKMP default profile

| Attribute    | Encryption | Integrity | Group | Authentication |
|--------------|------------|-----------|-------|----------------|
| Transform 1  | AES256     | SHA256    | 14    | Pre-shared     |
| Transform 2  | AES256     | SHA256    | 16    | Pre-shared     |
| Transform 3  | AES256     | SHA1      | 14    | Pre-shared     |
| Transform 4  | AES256     | SHA1      | 16    | Pre-shared     |
| Transform 5  | AES128     | SHA256    | 14    | Pre-shared     |
| Transform 6  | AES128     | SHA256    | 16    | Pre-shared     |
| Transform 7  | AES128     | SHA1      | 14    | Pre-shared     |
| Transform 8  | AES128     | SHA1      | 16    | Pre-shared     |
| Transform 9  | 3DES       | SHA256    | 14    | Pre-shared     |
| Transform 10 | 3DES       | SHA256    | 16    | Pre-shared     |
| Transform 11 | 3DES       | SHA1      | 14    | Pre-shared     |
| Transform 12 | 3DES       | SHA1      | 16    | Pre-shared     |

**Mode** Global Configuration

**Examples** To configure a custom ISAKMP profile for establishing ISAKMP SAs with a remote peer, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# transform 2 integrity sha1
encryption 3des group 5
```

To delete a custom profile, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp profile my_profile
```

**Related  
commands**

[dpd-interval](#)  
[dpd-timeout](#)  
[lifetime \(ISAKMP Profile\)](#)  
[transform \(ISAKMP Profile\)](#)  
[version \(ISAKMP\)](#)

**Validation  
Commands**

[show isakmp profile](#)

# debug isakmp

**Overview** Use this command to enable debugging ISAKMP.  
To disable debugging ISAKMP, see [no debug isakmp](#) or [undebug isakmp](#).

**Syntax** debug [crypto] isakmp [info|trace|all]

| Parameter | Description   |
|-----------|---|
| debug     | Debugging function.   |
| crypto    | Security specific command.  |
| isakmp    | Internet Security Association Key Management Protocol provides a common framework for key management implementations. |
| info      | Informational debug messages such as protocol events.   |
| trace     | Verbose debug messages including protocol events and message traces.  |
| all       | All debug enabled.  |

**Mode** Privileged Exec



**Examples** Figure 33-1: Example output from the **debug isakmp** command on the console.

```
awplus#debug isakmp info
awplus#terminal monitor
% Warning: Console logging enabled
awplus#show ipsec peer
21:03:42 awplus IMISH[30349]: show ipsec peer

10.2.0.10
IPSEC
  Selector: 0.0.0.0/0 0.0.0.0/0  tunnel1
  Profile: default
ISAKMP
  LocalID: 10.1.0.10
  RemoteID: 10.2.0.10
awplus#ping 192.168.1.2

PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
21:04:13 awplus iked: [DEBUG]: ike_pfkey.c:622:sadb_acquire_callback():
sadb_acquire_callback: seq=6 reqid=409
6 satype=96 sa_src=10.1.0.10[0] sa_dst=10.2.0.10[0] samode=229 selid=1
21:04:13 awplus iked: [DEBUG]: isakmp.c:918:isakmp_initiate(): new request (seq:6
spid:1 reqid:4096)
21:04:13 awplus iked: [DEBUG]: ikev2.c:758:ikev2_initiate(): creating new ike_sa
21:04:13 awplus iked: [DEBUG]: ike_sa.c:431:ikev2_allocate_sa():
ikev2_create_sa((nil), 10.1.0.10[500], 10.2.0
.10[500], 0x810b678)
21:04:13 awplus iked: [DEBUG]: ike_sa.c:434:ikev2_allocate_sa(): sa: 0x810d3a0
21:04:13 awplus iked: [DEBUG]: ikev2.c:800:ikev2_initiate(): child_sa: 0x810dd60
21:04:13 awplus iked: [DEBUG]: ikev2_child.c:139:ikev2_child_state_set(): child_sa
0x810dd60 state IDLING -> G
ETSPI
21:04:13 awplus iked: [DEBUG]: ike_pfkey.c:269:sadb_getspi(): sadb_getspi: seq=6,
satype=96
21:04:13 awplus iked: [DEBUG]: ike_pfkey.c:622:sadb_acquire_callback():
sadb_acquire_callback: seq=7 reqid=409
6 satype=96 sa_src=10.1.0.10[0] sa_dst=10.2.0.10[0] samode=229 selid=1
21:04:13 awplus iked: [DEBUG]: isakmp.c:918:isakmp_initiate(): new request (seq:7
spid:1 reqid:4096)
21:04:13 awplus iked: [DEBUG]: ikev2.c:800:ikev2_initiate(): child_sa: 0x810ec68
21:04:13 awplus iked: [DEBUG]: ikev2_child.c:139:ikev2_child_state_set(): child_sa
0x810ec68 state IDLING -> G
ETSPI

awplus#no debug isakmp
awplus#show debugging isakmp

ISAKMP Debugging status:
  ISAKMP Informational debugging is disabled
  ISAKMP Trace debugging is disabled
```

**Related commands** [no debug isakmp](#)  
[undebug isakmp](#)

# dpd-interval

**Overview** Use this command to specify the Dead Peer Detection (DPD) interval for an ISAKMP profile.

DPD is an IKE mechanism using a form of keep-alive to determine if a tunnel peer is still active.

The interval parameter specifies the amount of time the device waits for traffic from its peer before sending a DPD acknowledgment message.

Use the **no** variant to set the interval to its default (30 seconds).

**Syntax** `dpd-interval <10-86400>`  
`no dpd-interval`

| Parameter                     | Description                    |
|-------------------------------|--------------------------------|
| <code>&lt;10-86400&gt;</code> | Interval expressed in seconds. |

**Default** If you do not specify an interval, the default interval of 30 seconds applies.

**Mode** ISAKMP Profile Configuration

**Examples** To specify a DPD interval, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile  
awplus(config-isakmp-profile)# dpd-interval 20
```

To set the interval to its default, use the following commands:

```
awplus(config-isakmp-profile)# no dpd-interval
```

**Related commands** [crypto isakmp profile](#)

**Validation Commands** [show isakmp profile](#)

# dpd-timeout

**Overview** Use this command to specify a Dead Peer Detection (DPD) timeout for IKEv1. DPD is an IKE mechanism using a form of keep-alive to determine if a tunnel peer is still active. DPD timeout defines the timeout interval after which all connections to a peer are deleted in case of inactivity. This only applies to IKEv1, in IKEv2 the default retransmission timeout applies as every exchange is used to detect dead peers. Use the **no** variant to set the timeout to its default (150 seconds).

**Syntax** `dpd-timeout <10-86400>`  
`no dpd-timeout`

| Parameter                     | Description         |
|-------------------------------|---------------------|
| <code>&lt;10-86400&gt;</code> | Timeout in seconds. |

**Default** If you do not specify a timeout, the default timeout of 150 seconds applies.

**Mode** ISAKMP Profile Configuration

**Examples** To specify a DPD timeout for IKEv1, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile  
awplus(config-isakmp-profile)# dpd-timeout 200
```

To set the timeout to its default, use the following command:

```
awplus(config-isakmp-profile)# no dpd-timeout
```

**Related commands** [crypto isakmp profile](#)

**Related commands** [show isakmp profile](#)

# interface tunnel (IPsec)

**Overview** Use this command to create a tunnel interface or to enter Interface mode to configure an existing tunnel. Tunnel interfaces are identified by an index identifier that is an integer in the range from 0 through 65535.

Use the **no** variant of this command to remove a previously created tunnel interface.

**Syntax** `interface tunnel<0-65535>`  
`no interface tunnel<tunnel-index>`

| Parameter                    | Description   |
|------------------------------|---|
| <code>&lt;0-65535&gt;</code> | Specify a tunnel interface index identifier in the range from 0 to 65535. |

**Default** Tunnel interfaces do not exist.

**Mode** Global Configuration

**Usage notes** After you have created the tunnel interface, use the **tunnel mode** command to enable the tunnel.

Note that you need to designate a tunnel mode, tunnel source address, tunnel destination address, IP address of tunnel interface and use [tunnel protection ipsec \(IPsec\)](#) command to encrypt and authenticate the packets travelling though the tunnel.

**Examples** To configure an IPsec tunnel interface with index 100, enter the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel100
awplus(config-if)# tunnel mode ipsec ipv4
```

To remove the IPsec tunnel interface tunnel100, enter the commands below:

```
awplus# configure terminal
awplus(config)# no interface tunnel100
```

**Command changes** Version 5.4.7-2.1: increased range for **tunnel** index identifier.

# lifetime (IPsec Profile)

**Overview** Use this command to specify a lifetime for an IPsec SA.  
Lifetime measures how long the IPsec SA can be maintained before it expires. Lifetime prevents a connection from being used too long.  
Use the **no** variant to set the lifetime to default (28800 seconds).

**Syntax** `lifetime seconds <300-31449600>`  
`no lifetime seconds`

| Parameter                         | Description          |
|-----------------------------------|----------------------|
| <code>&lt;300-31449600&gt;</code> | Lifetime in seconds. |

**Default** If you do not specify a lifetime, the default lifetime of 28800 seconds (8 hours) applies.

**Mode** IPsec Profile Configuration

**Examples** To specify a lifetime for an IPsec SA, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile  
awplus(config-ipsec-profile)# lifetime seconds 400
```

To set the lifetime to its default, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile  
awplus(config-ipsec-profile)# no lifetime seconds
```

**Related commands** [crypto ipsec profile](#)

# lifetime (ISAKMP Profile)

**Overview** Use this command to specify a lifetime for an ISAKMP SA.  
Lifetime measures how long the ISAKMP SA can be maintained before it expires. Lifetime prevents a connection from being used too long.  
Use the **no** variant to set the lifetime to default (86400 seconds).

**Syntax** `lifetime <600-31449600>`  
`no lifetime`

| Parameter                         | Description          |
|-----------------------------------|----------------------|
| <code>&lt;600-31449600&gt;</code> | Lifetime in seconds. |

**Default** If you do not specify a lifetime, the default lifetime of 86400 seconds (8 hours) applies.

**Mode** ISAKMP Profile Configuration

**Examples** To specify a lifetime for an ISAKMP SA, use the following commands:

```
awplus(config)# configure isakmp profile my_profile  
awplus(config-isakmp-profile)# lifetime 700
```

To set the lifetime to its default, use the following commands:

```
awplus(config-isakmp-profile)# no lifetime
```

**Related commands** [crypto isakmp profile](#)

# no debug isakmp

**Overview** Use this command to disable debugging ISAKMP.  
To enable debugging ISAKMP, see [debug isakmp](#).

**Syntax** no [crypto] isakmp [info|trace|all]

| Parameter | Description   |
|-----------|---|
| no        | Disable debugging function.   |
| crypto    | Security specific.  |
| isakmp    | Internet Security Association Key Management Protocol provides a common framework for key management implementations. |
| info      | Informational debug messages such as protocol events.   |
| trace     | Verbose debug messages including protocol events and message traces.  |
| all       | All debug enabled.  |

**Mode** Privileged Exec

**Related commands** [debug isakmp](#)  
[undebug isakmp](#)

# pfs

**Overview** Use this command to enable PFS and set a Diffie-Hellman group for PFS in an IPsec profile.

Use the **no** variant to disable PFS.

**Syntax** `pfs {2|5|14|15|16|18}`  
`no pfs`

| Parameter | Description         |
|-----------|---------------------|
| 2         | 1024-bit MODP Group |
| 5         | 1536-bit MODP Group |
| 14        | 2048-bit MODP Group |
| 15        | 3072-bit MODP Group |
| 16        | 4096-bit MODP Group |
| 18        | 8192-bit MODP Group |

**Default** PFS is disabled.

**Mode** IPsec Profile Configuration

**Usage notes** Perfect Forward Secrecy (PFS) ensures generated keys, for example IPsec SA keys are not compromised if any other keys, for example, ISAKMP SA keys are compromised.

The specified PFS group must match the PFS group setting on the peer - especially when IKEv2 is used for ISAKMP SA negotiation. With IKEv2, if there is a PFS group mismatch an IPsec SA will be established and the tunnel will come up because PFS is not required for the initial child SA negotiation. However, when the IPsec SA rekeys it will fail due to the PFS group mismatch, and upon IPsec SA expiry the tunnel will no longer be able to carry traffic.

**Examples** To enable PFS and set a Diffie-Hellman group for PFS, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile  
awplus(config-ipsec-profile)# pfs 15
```

To disable PFS, use the following command:

```
awplus(config-ipsec-profile)# no pfs
```

**Related commands** [crypto ipsec profile](#)



**Validation** show ipsec profile  
**Commands**

# rekey

**Overview** Use this command to set the rekey policy for an IPsec profile. This policy will be used to make a decision or whether the SA will rekey at its expiry.

The options are **always**, **never**, and **on-demand**. The **on-demand** option makes its decision based on whether the link has seen any traffic since the SA's last rekey.

Use the **no** variant of this command to set the rekey policy back to its default of **always**.

**Syntax** rekey {always|never|on-demand}  
no rekey

| Parameter | Description   |
|-----------|---|
| always    | Always rekey this SA (default)                              |
| never     | Never rekey this SA   |
| on-demand | Only rekey this SA if it has been used since the last rekey |

**Default** By default, an IPsec SA will always rekey.

**Mode** IPsec Profile Configuration

**Usage notes** These options may be useful if you have a hub and spoke VPN topology and need to provision more than the maximum number of concurrent active VPNs supported by your device. **Never** and **on-demand** allow unused VPNs to be aged out, making more efficient use of the number of available VPNs.

**Example** To only rekey when traffic is detected over the interface, for the profile named 'myprofile', use the commands:

```
awplus# configure terminal
awplus(config)# crypto ipsec profile myprofile
awplus(config-ipsec-profile)# rekey on-demand
```

To reset the rekey policy back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# crypto ipsec profile myprofile
awplus(config-ipsec-profile)# no rekey
```

**Related commands** [crypto ipsec profile](#)  
[show ipsec profile](#)

**Command changes** Version 5.4.9-2.1: command added

# show debugging isakmp

**Overview** Use this command to show if debugging ISAKMP is enabled.

**Syntax** show debugging [crypto] isakmp

| Parameter | Description   |
|-----------|---|
| debugging | Debugging information.  |
| crypto    | Security specific command.  |
| isakmp    | Internet Security Association Key Management Protocol provides a common framework for key management implementations. |

**Mode** Privileged Exec

**Examples** To show if debugging ISAKMP is enabled, enter the command below:

```
awplus# show debugging isakmp
```

**Output** Figure 33-2: Example output from the **show debugging isakmp** command

```
awplus#show debugging isakmp
ISAKMP Debugging status:
  ISAKMP Informational debugging is enabled
  ISAKMP Trace debugging is disabled
```

# show interface tunnel (IPsec)

**Overview** Use this command to display status information of tunnels.

The tunnel remains inactive if no valid tunnel source or tunnel destination is configured.

**Syntax** `show interface tunnel< tunnel-index >`

| Parameter        | Description   |
|------------------|---|
| tunnel           | Specify this parameter to display tunnel status information of a given tunnel identified by the < tunnel-index > parameter. |
| < tunnel-index > | Specify a tunnel index in the range from 0 through 65535.   |

**Mode** Privileged Exec

**Examples** To display status information for IPsec tunnel "tunnel2", use the command:

```
awplus# show interface tunnel2
```

**Output** Figure 33-3: Example output from the **show interface tunnel** command

```
awplus#show interface tunnel2
Interface tunnel2
  Link is UP, administrative state is UP
  Hardware is Tunnel
  IPv4 address 192.168.1.1/24 point-to-point 192.168.1.255
  index 21 metric 1 mtu 1438
  <UP,POINT-TO-POINT,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  Tunnel source 10.1.0.10, destination 10.2.0.10
  Tunnel name local 10.1.0.10, remote 10.2.0.10
  Tunnel traffic selectors (ID, local, remote)
    1 192.168.2.0/24 192.168.3.0/24
    2 0.0.0.0/0 192.168.10.0/24
  Tunnel protocol/transport ipsec ipv4, key disabled, sequencing disabled
  Checksumming of packets disabled, path MTU discovery disabled
  Tunnel protection via IPsec (profile "default")
    input packets 11, bytes 924, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 03:23:10
```

**Related commands** [interface tunnel \(IPsec\)](#)

# show ipsec counters

**Overview** Use this command to show IPsec counters.

**Syntax** show [crypto] ipsec counters

| Parameter | Description  |
|-----------|--|
| crypto    | Security specific command.   |
| ipsec     | Internet Protocol Security defines the protection of IP packets using encryption and authentication. |
| counters  | Show IPsec transformation statistic.   |

**Mode** Privileged Exec

**Examples** To show IPsec counters, enter the command below:

```
awplus# show ipsec counters
```

**Output** Figure 33-4: Example output from the **show ipsec counters** command

```
awplus#show ipsec counters
Name                               Value
-----
InError                             0
InBufferError                       0
InHdrError                           0
InNoStates                           0
InStateProtoError                   0
InStateModeError                    0
InStateSeqError                     0
InStateExpired                       0
InStateMismatch                      0
InStateInvalid                       0
InTmpMismatch                        0
InNoPols                             0
InPolBlock                           0
InPolError                           0
OutError                             0
OutBundleGenError                   0
OutBundleCheckError                 0
OutNoStates                           0
OutStateProtoError                   0
OutStateModeError                    0
OutStateSeqError                     0
OutStateExpired                       0
OutPolBlock                           0
OutPolDead                           0
OutPolError                           0
FwdHdrError                          0
```

# show ipsec peer

**Overview** Use this command to show IPsec information on a per peer basis.

**Syntax** show [crypto] ipsec peer [<hostname>|<ipv4-addr>|<ipv6-addr>]

| Parameter   | Description  |
|-------------|--|
| crypto      | Security specific command.   |
| peer        | Remote endpoint.   |
| <hostname>  | Destination hostname.  |
| <ipv4-addr> | Destination IPv4 address. The IPv4 address uses the format A.B.C.D.  |
| <ipv6-addr> | Destination IPv6 address. The IPv6 address uses the format X:X::X:X. |

**Mode** Privileged Exec

**Examples** To show IPsec information on a per peer basis, enter the command below:

```
awplus# show ipsec peer 172.16.0.1
```

**Output** Figure 33-5: Example output from the **show ipsec peer** command

```
awplus#show ipsec peer 172.16.0.1
172.16.0.2
IPsec
  Selectors (local:remote)
    Address: 0.0.0.0/0 : 0.0.0.0/0
    Protocol: any:any
    Port: any:any
    Mark: 1:1
  Profile: default
  SAs:
    SPI (In:Out): ca865389:c9c7e3d3
    Selectors: 192.168.1.0/24 : 192.168.2.0/24
    Proto: ESP
    Mode: tunnel
    Encryption: AES256
    Integrity: SHA256
    Expires: 28796s
ISAKMP
  LocalID: 172.16.0.1
  RemoteID: 172.16.0.2
  SAs:
    Cookies (Initiator:Responder) 03071749781e5992:93f8457816d3d40d
    Ver: 2 Lifetime: 84569s State: Established
    Authentication: PSK Group: 14
    Encryption: AES256 NATT: no
    Integrity: SHA256 DPD: yes
```

# show ipsec policy

**Overview** Use this command to show IPsec policies.

**Syntax** show [crypto] ipsec policy

| Parameter | Description  |
|-----------|--|
| crypto    | Security specific command.   |
| ipsec     | Internet Protocol Security defines the protection of IP packets using encryption and authentication. |
| policy    | Policy.  |

**Mode** Privileged Exec

**Examples** To show IPsec policies, enter the command below:

```
awplus# show ipsec policy
```

**Output** Figure 33-6: Example output from the **show ipsec policy** command

```
awplus#show ipsec policy
Traffic Selector (addresses protocol ports interface)
  Profile          Peer
0.0.0.0/0 0.0.0.0/0  tunnel1
  default          10.2.0.10
```

# show ipsec profile

**Overview** Use this command to show IPsec default and custom profiles.

An IPsec profile consists of a set of parameters that are used by IPsec when establishing IPsec SAs with a remote peer. AlliedWare Plus provides default ISAKMP and IPsec profiles that contain a priority ordered set of transforms that are considered secure by the security community.

**Syntax** `show [crypto] ipsec profile [<profile_name>]`

| Parameter      | Description  |
|----------------|--|
| crypto         | Security specific.   |
| ipsec          | Internet Protocol Security defines the protection of IP packets using encryption and authentication. |
| profile        | An IPsec profile consists of a set of parameters that are used by IPsec SAs with a remote peer.      |
| <profile_name> | Custom profile name.   |

**Mode** Privileged Exec

**Examples** To show all IPsec profiles, including the default profile, use the following command:

```
awplus# show ipsec profile
```



**Output** Figure 33-7: Example output from the **show ipsec profile** command

```
awplus#show ipsec profile
IPsec Profile: default
  Replay-window: 32
  Rekey: Always
  Expiry: 8h
  PFS group: disabled
  Transforms:
  Protocol Integrity Encryption
    1 ESP SHA256 AES256
    2 ESP SHA1 AES256
    3 ESP SHA256 AES128
    4 ESP SHA1 AES128
    5 ESP SHA256 3DES
    6 ESP SHA1 3DES

IPsec Profile: my_profile
  Replay-window: 32
  Rekey: On Demand
  Expiry: 8h
  PFS group: disabled
  Transforms:
  Protocol Integrity Encryption
    2 ESP SHA1 3DES
```

**Examples** To show IPsec profile “my\_profile”, use the command:

```
awplus# show ipsec profile my_profile
```

**Output** Figure 33-8: Example output from the **show ipsec profile** command

```
awplus#show ipsec profile my_profile
IPsec Profile: my_profile
  Replay-window: 32
  Rekey: On Demand
  Expiry: 8h
  PFS group: disabled
  Transforms:
  Protocol Integrity Encryption
    2 ESP SHA1 3DES
```

**Related commands** [crypto ipsec profile](#)

# show ipsec sa

**Overview** Use this command to view the settings used by current security associations. SAs specify the Security Parameter Index (SPI), protocols, algorithms and keys for protecting a single flow of traffic between two IPsec peers. For more information about SA, see the [Internet Protocol Security \(IPSec\) Feature Overview and Configuration Guide](#).

**Syntax** show [crypto] ipsec sa

| Parameter | Description  |
|-----------|--|
| crypto    | Security specific command.   |
| ipsec     | Internet Protocol Security defines the protection of IP packets using encryption and authentication. |
| sa        | Security Association.  |

**Mode** Privileged Exec

**Examples** To view the settings used by current security associations, enter the command below:

```
awplus# show ipsec sa
```

**Output** Figure 33-9: Example output from the **show ipsec sa** command

```
awplus#show ipsec sa
```

| Peer      | SPI (in:out)<br>Encryption  | Mode<br>Integrity | Proto<br>PFS | Expires |
|-----------|-----------------------------|-------------------|--------------|---------|
| 10.0.0.20 | c2d8c150:7b24d3f5<br>AES256 | tunnel<br>SHA256  | ESP<br>-     | 28786s  |
| 10.0.0.22 | c6c2ad0d:0d008e3d<br>3DES   | tunnel<br>SHA1    | ESP<br>-     | 3582s   |
| 10.0.0.25 | cb36f9dd:cd87a834<br>AES128 | tunnel<br>SHA1    | ESP<br>2     | 28778s  |

# show isakmp counters

**Overview** Use this command to show ISAKMP counters.

**Syntax** show [crypto] isakmp counters

| Parameter | Description   |
|-----------|---|
| crypto    | Security specific command.  |
| isakmp    | Internet Security Association Key Management Protocol provides a common framework for key management implementations. |
| counters  | Show ISAKMP counters.   |

**Mode** Privileged Exec

**Examples** To show ISAKMP counters, enter the command below:

```
awplus# show isakmp counters
```

**Output** Figure 33-10: Example output from the **show isakmp counters** command

```
awplus#show isakmp counters
```

| Name             | Value |
|------------------|-------|
| ikeInitRekey     | 0     |
| ikeRspRekey      | 0     |
| ikeChildSaRekey  | 0     |
| ikeInInvalid     | 0     |
| ikeInInvalidSpi  | 0     |
| ikeInInitReq     | 0     |
| ikeInInitRsp     | 0     |
| ikeOutInitReq    | 0     |
| ikeOutInitRsp    | 0     |
| ikeInAuthReq     | 0     |
| ikeInAuthRsp     | 0     |
| ikeOutAuthReq    | 0     |
| ikeOutAuthRsp    | 0     |
| ikeInCrChildReq  | 0     |
| ikeInCrChildRsp  | 0     |
| ikeOutCrChildReq | 0     |
| ikeOutCrChildRsp | 0     |
| ikeInInfoReq     | 0     |
| ikeInInfoRsp     | 0     |
| ikeOutInfoReq    | 0     |
| ikeOutInfoRsp    | 0     |

# show isakmp key (IPsec)

**Overview** Use this command to show the ISAKMP pre-shared key. Pre-shared key authentication using optionally encrypted shared keys identified by hostname, IPv4 or IPv6 address. Pre-shared keys are not viewable and stored encrypted in the running-configuration.

**Syntax** `show [crypto] isakmp key`

| Parameter | Description   |
|-----------|---|
| crypto    | Security specific command.  |
| isakmp    | Internet Security Association Key Management Protocol provides a common framework for key management implementations. |
| key       | Pre-shared key.   |

**Mode** Privileged Exec

**Examples** To show ISAKMP pre-shared key, enter the command below:

```
awplus# show isakmp key
```

**Output** Figure 33-11: Example output from the **show isakmp key** command

```
awplus#show isakmp key
Hostname/IP address      Key
10.2.0.10                mytunnelkey
```

# show isakmp peer

**Overview** Use this command to show ISAKMP profile and key status for ISAKMP peers.

**Syntax** `show isakmp peer [<hostname>|<ipv4-addr>|<ipv6-addr>]`

| Parameter   | Description  |
|-------------|--|
| <hostname>  | Destination hostname.  |
| <ipv4-addr> | Destination IPv4 address. The IPv4 address uses the format A.B.C.D.  |
| <ipv6-addr> | Destination IPv6 address. The IPv6 address uses the format X:X::X:X. |

**Mode** Privileged Exec

**Examples** To show ISAKMP profile and key status for ISAKMP peers, use the following command:

```
awplus# show isakmp peer
```

**Output** Figure 33-12: Example output from the **show isakmp peer** command

```
awplus#show isakmp peer
Peer                               Profile (* incomplete)           Key
-----
example.com                        LEGACY                           Not Found
2.2.2.2                             default                          PSK
1.1.1.1                             SECURE                           PSK
```

**Related commands** [crypto isakmp peer](#)

**Command changes** Version 5.4.7-0.1: Parameter <hostname> added for DDNS feature.

# show isakmp profile

**Overview** Use this command to show ISAKMP default and custom profiles.

**Syntax** show [crypto] isakmp profile [<profile\_name>]

| Parameter      | Description          |
|----------------|----------------------|
| <profile_name> | Custom profile name. |

**Mode** Privileged Exec

**Examples** To show ISAKMP profiles, including the default profile, use the command:

```
awplus# show isakmp profile
```

**Output** Figure 33-13: Example output from the **show isakmp profile** command

```
awplus#show isakmp profile
ISAKMP Profile: default
  Version:      IKEv2
  Authentication: PSK
  Expiry:       24h
  DPD Interval: 30s
  Transforms:
    Integrity  Encryption  DH Group
    1  SHA256   AES256     14
    2  SHA256   AES256     16
    3  SHA1     AES256     14
    4  SHA1     AES256     16
    5  SHA256   AES128     14
    6  SHA256   AES128     16
    7  SHA1     AES128     14
    8  SHA1     AES128     16
    9  SHA256   3DES      14
   10  SHA256   3DES      16
   11  SHA1     3DES      14
   12  SHA1     3DES      16

ISAKMP Profile: my_profile
  Version:      IKEv2
  Authentication: PSK
  Expiry:       24h
  DPD Interval: 30s
  Transforms:
    Integrity  Encryption  DH Group
    2  SHA1     3DES      5
```

**Examples** To show ISAKMP profile “my\_profile”, use the command:

```
awplus# show isakmp profile my_profile
```

**Output** Figure 33-14: Example output from the **show isakmp profile** command

```
awplus#show isakmp profile my_profile
ISAKMP Profile: my_profile
Version:          IKEv2
Authentication:   PSK
Expiry:           24h
DPD Interval:     30s
Transforms:
  Integrity      Encryption  DH Group
  2              3DES       5
```

**Related commands** [crypto isakmp profile](#)

# show isakmp sa

**Overview** Use this command to show current IKE security associations at a peer.

**Syntax** show [crypto] isakmp sa

| Parameter | Description   |
|-----------|---|
| crypto    | Security specific command.  |
| isakmp    | Internet Security Association Key Management Protocol provides a common framework for key management implementations. |
| sa        | Security Association.   |

**Mode** Privileged Exec

**Examples** To show current IKE security associations at a peer, enter the command below:

```
awplus# show isakmp sa
```

**Output** Figure 33-15: Example output from the **show isakmp sa** command

```
awplus#show isakmp sa
```

| Peer      | Cookies (initiator:responder)<br>Encryption Integrity Group | Auth<br>DPD | Ver<br>NATT | Expires<br>State      |
|-----------|---|-------------|-------------|-----------------------|
| 10.0.0.20 | f93c2717a1ece407:972bc0c77344d7a4<br>AES256 SHA256 2        | PSK<br>yes  | 1<br>no     | 78340s<br>Established |
| 10.0.0.22 | ccb7f90b54945375:2642525bd20f3428<br>3DES SHA1 2            | PSK<br>yes  | 1<br>no     | 3334s<br>Established  |
| 10.0.0.25 | bd0efef134c86656:d46d01b72b46444<br>AES128 SHA1 2           | PSK<br>yes  | 1<br>no     | 819s<br>Established   |



# transform (IPsec Profile)

**Overview** Use this command to create an IPsec profile transform, which specifies the encryption and authentication algorithms used to protect data.

Use the **no** variant to delete a previously created transform.

**Syntax** `transform <1-255> protocol esp integrity {sha1|sha256|sha512}  
encryption {3des|aes128|aes192|aes256|null}`  
`no transform <1-255>`

| Parameter | Description  |
|-----------|--|
| <1-255>   | Transform priority (1 is the highest)  |
| sha1      | Secure Hash Standard with 160-bit digest size  |
| sha256    | Secure Hash Standard with 256-bit digest size  |
| sha512    | Secure Hash Standard with 512 bit digest size  |
| 3des      | Triple DES symmetric key block cipher with a 168-bit key   |
| aes128    | Advanced Encryption Standard symmetric key block cipher with a 128-bit key   |
| aes192    | Advanced Encryption Standard symmetric key block cipher with a 192-bit key   |
| aes256    | Advanced Encryption Standard symmetric key block cipher with a 256-bit key   |
| null      | No encryption. This option is not intended for use in a live network. It should only be used for testing purposes. |

**Default** By default, an IPsec profile has no transforms and so will not be active.

**Mode** IPsec Profile Configuration

**Examples** To configure an IPsec profile transform, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile  
awplus(config-ipsec-profile)# transform 2 protocol esp  
integrity sha1 encryption 3des
```

To delete a created transform, use the following command:

```
awplus(config-ipsec-profile)# no transform 2
```

**Related commands** [crypto ipsec profile](#)

**Validation Commands** [show ipsec profile](#)

# transform (ISAKMP Profile)

**Overview** Use this command to create an ISAKMP profile transform which specifies the encryption and authentication algorithms used to protect data in the tunnel.

Use the **no** variant to delete a previously created transform.

**Syntax** transform <1-255> integrity {sha1|sha256|sha512} encryption {3des|aes128|aes192|aes256} group {2|5|14|15|16|18}  
no transform <1-255>

| Parameter | Description  |
|-----------|--|
| <1-255>   | Transform priority (1 is the highest)                                      |
| sha1      | Secure Hash Standard with 160-bit digest size                              |
| sha256    | Secure Hash Standard with 256-bit digest size                              |
| sha512    | Secure Hash Standard with 512 bit digest size                              |
| 3des      | Triple DES symmetric key block cipher with a 168-bit key                   |
| aes128    | Advanced Encryption Standard symmetric key block cipher with a 128-bit key |
| aes192    | Advanced Encryption Standard symmetric key block cipher with a 192-bit key |
| aes256    | Advanced Encryption Standard symmetric key block cipher with a 256-bit key |
| group     | Diffie-Hellman group   |
| 2         | 1024-bit MODP Group  |
| 5         | 1536-bit MODP Group  |
| 14        | 2048-bit MODP Group  |
| 15        | 3072-bit MODP Group  |
| 16        | 4096-bit MODP Group  |
| 18        | 8192-bit MODP Group  |

**Default** By default, an ISASMP profile has no transforms and so will not be active.

**Mode** ISAKMP Profile Configuration

**Examples** To create an ISAKMP profile transform, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile  
awplus(config-isakmp-profile)# transform 2 integrity sha1  
encryption 3des group 5
```

To delete a created transform, use the following command:

```
awplus(config-isakmp-profile)# no transform 2
```

**Related commands** [crypto isakmp profile](#)

# tunnel destination (IPsec)

**Overview** Use this command to specify a destination IPv4 or IPv6 address or destination network name for the remote end of the tunnel.

Use the **no** variant of this command to remove a configured tunnel destination address.

**Syntax** tunnel destination {<WORD>|<ipv4-address>|<ipv6-address>}  
no tunnel destination {<WORD>|<ipv4-address>|<ipv6-address>}

| Parameter      | Description   |
|----------------|---|
| <WORD>         | Destination network name or "dynamic". The "dynamic" parameter allows you to specify a dynamic IP address for the remote endpoint. The dynamic IP address can be obtained, for example, via DHCP. |
| <ipv4-address> | Destination IPv4 address. The IPv4 address uses the format A.B.C.D.   |
| <ipv6-address> | Destination IPv6 address. The IPv4 address uses the format X:X::X:X.  |

**Mode** Interface Configuration

**Examples** To configure a destination IPv4 address for IPsec tunnel45, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination 192.0.3.1
```

To configure a destination IPv6 address for IPsec tunnel45, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel destination 2001:0db8::
```

To configure a destination network name for IPsec tunnel45, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination www.example.com
```

To configure a dynamic IP address for the tunnel destination, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination dynamic
```

To remove the destination address of IPsec tunnel45, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# no tunnel destination 192.0.3.1
```

**Related commands** [tunnel source \(IPsec\)](#)

# tunnel local name (IPsec)

**Overview** Use this command to specify an IPsec tunnel hostname to send to the peer for authentication when you apply [tunnel protection ipsec \(IPsec\)](#) to encrypt the packets and configure an ISAKMP key.

Use the **no** variant of this command to remove a previously configured IPsec tunnel hostname.

**Syntax** tunnel local name *<local-name>*  
no tunnel local name

| Parameter                 | Description             |
|---------------------------|-------------------------|
| <i>&lt;local-name&gt;</i> | Source tunnel hostname. |

**Default** The default tunnel local name is the IP address of tunnel source.

**Mode** Interface Configuration

**Examples** To configure the tunnel local name office1 for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel local name office1
```

To remove a configured tunnel local name for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel local name
```

**Related commands** [tunnel remote name \(IPsec\)](#)

# tunnel local selector

**Overview** Use this command to specify a local subnet for a traffic selector pair.

Use the **no** variant of this command to unset the local subnet for the traffic selector pair so that it matches all sources, i.e. 0.0.0.0/0 or ::/0 for IPv4 and IPv6, respectively. When local and remote subnets for a traffic selector pair are both unset, the traffic selector pair is removed.

**Syntax** tunnel local selector [*<traffic-selector-ID>*]  
{*<ipv4-subnet>* | *<ipv6-subnet>*}  
no tunnel local selector [*<traffic-selector-ID>*]

| Parameter                          | Description  |
|------------------------------------|--|
| <i>&lt;traffic-selector-ID&gt;</i> | Optional traffic selector ID from 1 through 65535. The default is 1. |
| <i>&lt;ipv4-subnet&gt;</i>         | IPv4 subnet in the format A.B.C.D/M.                                 |
| <i>&lt;ipv6-subnet&gt;</i>         | IPv6 subnet in the format of X:X::X:X/M                              |

**Default** When no traffic selector pairs are configured there is an implicit traffic selector pair, where the local and remote subnets are 0.0.0.0/0 or ::/0 depending on the tunnel IPsec mode.

**Mode** Interface configuration

**Usage notes** A traffic selector pair is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote subnets. When the local selector is specified but the remote selector is not, the selector pair implicitly matches all destinations.

**Examples** To specify an IPv4 destination address as the traffic selector for the traffic to match for tunnel0, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth1
awplus(config-if)# tunnel destination 10.0.0.2
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel local selector 192.168.1.0/24
awplus(config-if)# tunnel remote selector 192.168.2.0/24
```

To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 192.168.1.0/24  
awplus(config-if)# tunnel remote selector 5 192.168.2.0/24
```

To specify an IPv6 source address as the traffic selector for the traffic to match for tunnel0, use the commands below:

```
awplus# configure terminal  
awplus(config)# interface tunnel0  
awplus(config-if)# tunnel source eth1  
awplus(config-if)# tunnel destination 2001:db8:10::1  
awplus(config-if)# tunnel local name office  
awplus(config-if)# tunnel mode ipsec ipv6  
awplus(config-if)# tunnel local selector 2001:db8:1::/64  
awplus(config-if)# tunnel remote selector 2001:db8:2::/64
```

To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 2001:db8:1::/64  
awplus(config-if)# tunnel remote selector 5 2001:db8:2::/64
```

To unset the destination traffic selector for the traffic selector pair with ID 1, for tunnel 6, use the commands:

```
awplus# configure terminal  
awplus(config)# interface tunnel6  
awplus(config-if)# no tunnel remote selector  
  
or  
  
awplus(config-if)# no tunnel remote selector 1
```

**Related commands**

- [tunnel remote selector](#)
- [tunnel selector paired](#)
- [show interface tunnel \(IPsec\)](#)



# tunnel mode ipsec

**Overview** Use this command to configure the encapsulation tunneling mode to use.  
Use the **no** variant of this command to remove an established tunnel.

**Syntax** tunnel mode ipsec {ipv4|ipv6}  
no tunnel mode

| Parameter  | Description       |
|------------|-------------------|
| ipsec ipv4 | IPv4 IPsec tunnel |
| ipsec ipv6 | IPv6 IPsec tunnel |

**Default** Virtual tunnel interfaces have no mode set.

**Mode** Interface Configuration

**Usage notes** A tunnel will not become operational until it is configured with this command.

**Examples** To configure IPsec in IPv4 tunnel mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel mode ipsec ipv4
```

To remove the configured IPsec tunnel mode for tunnel6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel mode
```

# tunnel protection ipsec (IPsec)

**Overview** Use this command to enable IPsec protection for packets encapsulated by this tunnel.

Use the **no** variant to disable IPsec protection.

**Syntax** tunnel protection ipsec [profile <profile\_name>]  
no tunnel protection ipsec

**Default** IPsec protection for packets encapsulated by tunnel is disabled. If no custom profile is specified, the default profile is used.

| Parameter      | Description  |
|----------------|--|
| <profile_name> | Custom profile name. You can use the <a href="#">crypto ipsec profile</a> command to create custom profiles. |

**Mode** Interface Configuration

**Usage notes** IPsec mode tunnels (IPv4 and IPv6) require this command for them to work.

**Examples** To enable IPsec protection by using default profile, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# tunnel protection ipsec
```

To enable IPsec protection by using a custom profile, use the following commands:

```
awplus(config)# interface tunnel14
awplus(config-if)# tunnel protection ipsec profile
my_profile
```

To disable IPsec protection for packets encapsulated by tunnel14, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# no tunnel protection ipsec
```

**Related commands** [crypto ipsec profile](#)

# tunnel remote name (IPsec)

**Overview** Use this command to specify a tunnel remote name to authenticate the tunnel's remote peer device when you apply [tunnel protection ipsec \(IPsec\)](#) to encrypt the packets and configure an ISAKMP key.

Use the **no** variant of this command to remove a previously configured tunnel remote name.

**Syntax** tunnel remote name *<remote-name>*  
no tunnel local name

| Parameter                  | Description                 |
|----------------------------|-----------------------------|
| <i>&lt;remote-name&gt;</i> | Destination tunnel hostname |

**Default** The default tunnel remote name is the IP address of tunnel destination.

**Mode** Interface Configuration

**Examples** To configure tunnel remote name office2 for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel remote name office2
```

To remove a configured tunnel local name for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel remote name
```

**Related commands** [tunnel local name \(IPsec\)](#)

# tunnel remote selector

**Overview** Use this command to specify a destination subnet for a traffic selector pair.

Use the **no** variant of this command to unset the remote subnet for a traffic selector pair so that it matches all destinations, i.e. 0.0.0.0/0 or ::/0 for IPv4 and IPv6, respectively. When local and remote subnets for a traffic selector pair are both unset, the traffic selector pair is removed.

**Syntax** tunnel remote selector [*<traffic-selector-ID>*]  
{*<IPv4-subnet>* | *<IPv6-subnet>*}  
no tunnel remote selector [*<traffic-selector-ID>*]

| Parameter                          | Description   |
|------------------------------------|---|
| <i>&lt;traffic-selector-ID&gt;</i> | Traffic selector ID from 1 through 65535. If not specified the default value 1 is used. |
| <i>&lt;ipv4-subnet&gt;</i>         | IPv4 subnet in the format A.B.C.D/M.  |
| <i>&lt;ipv6-subnet&gt;</i>         | IPv6 subnet in the format of X:X::X:X/M   |

**Default** When no traffic selector pairs are configured there is an implicit traffic selector pair, where the local and remote subnets are 0.0.0.0/0 or ::/0 depending on the tunnel IPsec mode.

**Mode** Interface configuration

**Usage notes** A traffic selector pair is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote subnets. When the remote selector is specified but the local selector is not, the selector pair implicitly matches all sources.

**Examples** To specify an IPv4 destination address as the traffic selector for the traffic to match for tunnel0, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth1
awplus(config-if)# tunnel destination 10.0.0.2
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel local selector 192.168.1.0/24
awplus(config-if)# tunnel remote selector 192.168.2.0/24
```

When no traffic selector ID is specified the default ID value is used. By specifying a traffic selector ID, additional selector pairs can be configured.

To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 192.168.1.0/24  
awplus(config-if)# tunnel remote selector 5 192.168.2.0/24
```

To specify an IPv6 source address as the traffic selector for the traffic to match for tunnel0, use the commands below:

```
awplus# configure terminal  
awplus(config)# interface tunnel0  
awplus(config-if)# tunnel source eth1  
awplus(config-if)# tunnel destination 2001:db8:10::1  
awplus(config-if)# tunnel local name office  
awplus(config-if)# tunnel mode ipsec ipv6  
awplus(config-if)# tunnel local selector 2001:db8:1::/64  
awplus(config-if)# tunnel remote selector 2001:db8:2::/64
```

To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 2001:db8:1::/64  
awplus(config-if)# tunnel remote selector 5 2001:db8:2::/64
```

To unset the destination traffic selector for the traffic selector pair with ID 1, for tunnel6, use the commands:

```
awplus# configure terminal  
awplus(config)# interface tunnel6  
awplus(config-if)# no tunnel remote selector
```

or

```
awplus(config-if)# no tunnel remote selector 5
```

**Related commands**

- [tunnel local selector](#)
- [tunnel selector paired](#)
- [show interface tunnel \(IPsec\)](#)

# tunnel security-reprocessing

**Overview** Use this command to enable stream security reprocessing on all tunnel interfaces.

Use the **no** variant of this command to disable security reprocessing on all tunnel interfaces.

Note that tunnel security reprocessing increases the load on your device and reduces throughput. This is because traffic is processed twice through the DPI engine. Therefore, it should only be enabled if your solution requires it.

**Syntax** tunnel security-reprocessing  
no tunnel security-reprocessing

**Default** Security reprocessing is disabled by default.

**Mode** Global Configuration

**Usage notes** Use this command when you need to reinspect the traffic in a tunnel terminating on the device using stream UTM features after tunnel headers and encryption have been removed. For a configuration example using this command, see the [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#).

**Example** To enable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# tunnel security-reprocessing
```

To disable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# no tunnel security-reprocessing
```

**Related commands** [show interface tunnel \(IPsec\)](#)

**Command changes** Version 5.4.8-0.2: command added

# tunnel selector paired

**Overview** Use this command when multiple selector pairs are configured. This command forces ISAKMP to use strict pairing and therefore create separate Phase 2 IPsec SAs between pairs of source and destination selectors, based on selector ID.

Use the **no** variant of this command to stop forcing strict selector ID pairing.

**Syntax** tunnel selector paired

**Default** Disabled

**Mode** Interface mode for a tunnel

**Usage notes** When this command is disabled, if you specify address selectors, the tunnel can permit any combination of matching sources and/or destinations. While this conforms to the RFC, it may not be the expected behavior and may cause the IPsec SA to either fail negotiation or fail to pass traffic correctly.

This command forces ISAKMP to create individual IPsec SAs for each pair of source and destination selectors that have the same selector ID. Only traffic that matches a selector pair is permitted to flow via the associated SA.

**Example** To create a tunnel between 172.16.1.0/24 and 172.16.2.0/24, and also between 172.16.1.0/24 and any other destination, use the following tunnel selector commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel local selector 2 172.16.1.0/24
awplus(config-if)# tunnel remote selector 2 172.16.2.0/24
awplus(config-if)# tunnel local selector 3 172.16.1.0/24
awplus(config-if)# tunnel remote selector 3 0.0.0.0/0
awplus(config-if)# tunnel selector paired
```

**Related commands** [tunnel local selector](#)  
[tunnel remote selector](#)  
[show interface tunnel \(IPsec\)](#)

**Command changes** Version 5.4.8-1.1: command added

# tunnel source (IPsec)

**Overview** Use this command to specify an IPv4 or IPv6 source address or interface name for packets being encapsulated in the IPsec tunnel. The source address should be an existing IPv4 address or IPv6 address or interface name configured for an interface.

Use the **no** variant of this command to remove a tunnel source address for a tunnel interface.

**Syntax** tunnel source {<interface-name> | <ipv4-address> | <ipv6-address>}  
no tunnel source  
{<interface-name> | <ipv4-address> | <ipv6-address>}

| Parameter      | Description                                |
|----------------|--|
| <interface>    | Interface name.                            |
| <ipv4-address> | The IPv4 address uses the format A.B.C.D.  |
| <ipv6-address> | The IPv6 address uses the format X:X::X:X. |

**Mode** Interface Configuration

**Examples** To configure a source IPv4 address for IPsec tunnel45, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel source 192.168.1.1
```

To configure a source IPv6 address for IPsec tunnel45, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel source 2001:db8::
```

To configure a source interface for IPsec tunnel45, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel source eth1
```

To remove the source address of IPsec tunnel45, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# no tunnel source 192.168.1.1
```



**Related commands** [tunnel destination \(IPsec\)](#)

# undebg isakmp

**Overview** Use this command to disable debugging ISAKMP.

To enable debugging ISAKMP, see [debug isakmp](#).

**Syntax** undebg [crypto] isakmp [info|trace|all]

| Parameter | Description   |
|-----------|---|
| undebg    | Disable debugging function.   |
| crypto    | Security specific command.  |
| isakmp    | Internet Security Association Key Management Protocol provides a common framework for key management implementations. |
| info      | Informational debug messages such as protocol events.   |
| trace     | Verbose debug messages including protocol events and message traces.  |
| all       | All debug enabled.  |

**Mode** Privileged Exec

**Related commands** [debug isakmp](#)  
[no debug isakmp](#)

# version (ISAKMP)

**Overview** Use this command to set the ISAKMP protocol version.  
Use the **no** variant to set the protocol version to default (IKEv2).

**Syntax** `version {1 mode {aggressive|main} | 2}`  
`no version`

| Parameter  | Description   |
|------------|---|
| 1          | IKEv1   |
| main       | IKEv1 Main mode. An IKE session begins with the initiator and recipient sending three two-way exchanges to define what encryption and authentication protocols are acceptable, how long keys should remain active, and whether perfect forward secrecy should be enforced. Main mode uses more packets for the process than Aggressive mode, but Main mode is considered more secure. |
| aggressive | IKEv1 Aggressive mode. The initiator and recipient accomplish the same objectives, but in only two exchanges.   |
| 2          | IKEv2   |

**Default** If you do not specify the version, the default version is IKEv2

**Mode** IPsec ISAKMP Configuration

**Examples** To set the ISAKMP protocol version of profile "my\_profile" to IKEv1 main mode, use the following commands:

```
awplus(config)# configure isakmp profile my_profile  
awplus(config-isakmp-profile)# version 1 mode main
```

To set the version to its default, use the following command:

```
awplus# no version
```

**Related commands** [crypto isakmp profile](#)

**Validation Commands** [show isakmp profile](#)

# 34

# Transitioning IPv4 to IPv6 Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure Light Weight 4 over 6 and MAP E.

Many ISPs have migrated from IPv4 to IPv6 networks. However, many customers are still using IPv4 facilities. IPv6 transition technologies, such as Light Weight 4 over 6 (LW4o6) and MAP-E, provide interoperability between IPv4 and IPv6 networks. This enables ISPs with IPv6 networks to provide Internet connectivity to customers with IPv4 facilities.

MAP-E provides a mechanism for mapping between an IPv4 prefix or IPv4 address or IPv4 shared address and an IPv6 address. It also uses the encapsulation mode described in RFC 2473 (IPv6 Tunneling) to transport IPv4 packets over an IPv6 network.

Dual-Stack Lite (DS-Lite) (RFC 6333) describes an architecture for transporting IPv4 packets over an IPv6 network. This chapter describes an extension to DS-Lite called "Lightweight 4over6", which moves the Network Address and Port Translation (NAPT) function from the centralized DS-Lite tunnel concentrator to the tunnel client located in the Customer Premises Equipment (CPE).

This removes the requirement for a Carrier Grade NAT function in the tunnel concentrator and reduces the amount of centralized state that must be held to a per-subscriber level. In order to delegate the NAPT function and make IPv4 address sharing possible, port-restricted IPv4 addresses are allocated to the CPEs.

- Useful Terms**
- **Softwire:** A tunnel between two IPv6 end-points to carry IPv4 packets or two IPv4 end-points to carry IPV6 packets.
  - **B4:** Softwire at the customer end that encapsulates native packets and tunnels them to a softwire concentrator (AFTR) at the service provider.
  - **AFTR:** Softwire that decapsulates the packets received from a softwire B4 and sends them to their destination.

For more information, see the [Transitioning IPv4 to IPv6 Feature Overview and Configuration Guide](#).

- Command List**
- `br-address (software)` on page 1366
  - `mesh-mode` on page 1367
  - `method (software)` on page 1368
  - `rule (software)` on page 1369
  - `show running-config software-configuration` on page 1371
  - `show software-configuration` on page 1372
  - `software-configuration` on page 1374
  - `tunnel security-reprocessing` on page 1375
  - `tunnel destination (DS-Lite)` on page 1376
  - `tunnel mode ds-lite` on page 1377
  - `tunnel mode lw4o6` on page 1378
  - `tunnel mode map-e` on page 1379
  - `tunnel software` on page 1380
  - `upstream-interface` on page 1381

# br-address (software)

**Overview** Use this command to specify the IPv6 address of the MAP-E Border Router. Note, before using this command you must configure the command **method (Software Configuration)** with the **static** parameter.

Use the **no** variant of this command to remove the MAP-E Border Router address configuration.

**Syntax** `br-address <ipv6-address>`  
`no br-address`

| Parameter                         | Description                         |
|-----------------------------------|-------------------------------------|
| <code>&lt;ipv6-address&gt;</code> | IPv6 address of MAP-E Border Router |

**Default** Not set.

**Mode** SoftWire Configuration

**Example** To configure 'swconfig' to the software configuration MAP-E Border Router IPv6 address, use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# br-address 2001::1
```

To remove the MAP-E Border Router IPv6 address configuration for 'swconfig', use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# no br-address
```

**Related commands** [show software-configuration](#)

**Command changes** Version 5.4.9-0.1: command added

# mesh-mode

**Overview** Use this command to enable mesh-mode. Mesh-mode enables softwire tunnels to work with devices that share the same IP address at the tunnel endpoint.

Use the **no** variant of this command to disable mesh-mode.

**Syntax** mesh-mode  
no mesh-mode

**Default** No mesh-mode.

**Mode** SoftWire Configuration

**Usage notes** Softwire tunnels may require communication with endpoints sharing the same IP address. The CPU resource required to support this is significant, so this command enables this support.

**Example** To configure a softwire named 'demo' to communicate with endpoints that share the same IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# softwire-configuration demo
awplus(config-softwire)# mesh-mode
```

**Related commands** show softwire-configuration  
softwire-configuration

**Command changes** Version 5.4.9-0.1: command added

# method (software)

**Overview** Use this command to specify the configuration method (or source) for a software configuration. The configuration method can be either static or DHCP.

Use the **no** variant of this command to remove a configured method.

**Syntax** `method {static|dhcp}`  
`no method`

| Parameter           | Description                                     |
|---------------------|---|
| <code>static</code> | Software configuration is statically configured |
| <code>dhcp</code>   | Software configuration is acquired through DHCP |

**Default** Not set.

**Mode** SoftWire Configuration

**Example** To set the 'swconfig' software configuration method to **static**, use the commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# method static
```

To set the 'swconfig' software configuration method to **DHCP**, use the commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# method dhcp
```

To remove the software configuration method from 'swconfig', use the commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# no method
```

**Related commands** [show software-configuration](#)  
[rule \(software\)](#)

**Command changes** Version 5.4.9-0.1: command added



# rule (software)

**Overview** Use this command to statically configure a MAP rule. Note, before using this command you must configure the command **method (Software Configuration)** with the **static** parameter.

You would normally obtain the values to use in this command from your ISP.

Use the **no** variant of this command to remove a MAP rule configuration.

**Syntax**

```
rule <0-65535> ipv4-prefix <ipv4-prefix> ipv6-prefix  
<ipv6-prefix> psid-length <0-15> psid <psid-value> [offset  
<0-16>] [forwarding]  
  
rule <0-65535> ipv4-prefix <ipv4-prefix> ipv6-prefix  
<ipv6-prefix> ea-length <0-48> [offset <0-16>] [forwarding]  
  
no rule <0-65535>
```

| Parameter                 | Description   |
|---------------------------|---|
| rule <0-65535>            | Rule ID is an integer in the range <1-65535>  |
| ipv4-prefix <ipv4-prefix> | IPv4 prefix (e.g. 192.0.2.0/24)   |
| ipv6-prefix <ipv6-prefix> | IPv6 prefix (e.g. 2001:db8::/32)  |
| ea-length <0-48>          | Embedded address length is an integer in the range <0-48>.  |
| psid-length <0-15>        | Port Set ID (PSID) length is an integer in the range <0-15>, the default length is 0.   |
| psid <psid-value>         | Port Set ID (PSID) value is either decimal <0-65535> or hexadecimal with a leading 0x. Different PSID values guarantee non-overlapping port sets. |
| offset <0-16>             | Port Set ID (PSID) offset is an integer in the range <0-16>.  |
| forwarding                | Indicates if this rule is a Forwarding Mapping Rule (FMR). Otherwise, this is only used as a Basic Mapping Rule (BMR)                             |

**Default** Not set.

**Mode** SoftWire Configuration

**Example** To configure a MAP rule 1 and MAP rule 2 in Software Configuration 'swconfig', use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# rule 1 ipv4-prefix 192.0.2.0/24
ipv6-prefix 2001:db8:1::/48 ea-length 16 forwarding
awplus(config-software)# rule 2 ipv4-prefix 192.0.2.23/32
ipv6-prefix 2001:db8:1:1781::/64 psid-length 8 psid 129
```

These two example rules above produce the same resulting IPv4 address and PSID if the IPv6 subnet on the upstream interface is 2001:db8:1:1781::/64.

To the remove rule 1 in Software Configuration 'swconfig', use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# no rule 1
```

**Related commands** [method \(software\)](#)  
[show software-configuration](#)

**Command changes** Version 5.4.9-0.1: command added

# show running-config software-configuration

**Overview** Use this command to display the running configuration information for a software configuration.

**Syntax** `show running-config software-configuration`  
`<software-config-name>`  
`show running-config software-configuration`

| Parameter                                 | Description                                      |
|---|--|
| <code>&lt;software-config-name&gt;</code> | The name assigned for the Software Configuration |

**Mode** Privileged Exec

**Example** To show the running configuration for **all** software configuration, use the following command:

```
awplus# show running-config software-configuration
```

To show the running configuration for software configuration 'swconfig1', use the following command:

```
awplus# show running-config software-configuration swconfig1
```

**Output** Figure 34-1: Example output from **show running-config software-configuration**

```
awplus#show running-config software-configuration
software-configuration swconfig1
  method static
  map-version rfc
  br-address 2001:db8:1234:5678::1
  rule 10 ipv4-prefix 192.168.1.0/24 ipv6-prefix 2001:db8:1000::/48 ea-length 16 forwarding
  rule 20 ipv4-prefix 192.168.2.0/24 ipv6-prefix 2001:db8:2000::/48 ea-length 16 forwarding
  rule 30 ipv4-prefix 192.168.3.0/24 ipv6-prefix 2001:db8:3000::/48 ea-length 16 forwarding
!
software-configuration swconfig2
  method dhcp
  upstream-interface eth1
!
```

**Related commands** [software-configuration](#)

**Command changes** Version 5.4.9-0.1: command added

# show software-configuration

**Overview** Use this command to show information about the configuration state of software configuration. You can show information for all software configurations or define a specific configuration for display.

**Syntax** `show software-configuration <software-config-name>`  
`show software-configuration`

| Parameter                                 | Description                                 |
|---|---|
| <code>&lt;software-config-name&gt;</code> | Name assigned to the Software Configuration |

**Mode** Privileged Exec

**Example** To show information about the configuration state of **all** software configuration, use the command:

```
awplus# show software-configuration
```

To show information about the configuration state of software configuration 'swconfig1', use the command:

```
awplus# show software-configuration swconfig1
```

**Output** Figure 34-2: Example output for a Static MAP-E software configuration

```
awplus#show software-configuration swconfig1

Software Configuration: swconfig1

Configuration Source: static
Upstream Interface: eth1
MAP-E Version: rfc
No LW4o6 Configuration

Border Relay Device: 2001:db8::1
Rule 0
  IPv4-prefix: 192.0.2.0/24
  IPv6-prefix: 2001:db8::/32
  Embedded address length: 16
  Forwarding: enabled
  PSID offset: default
  PSID length: default
  PSID: default (0x0)
```

Figure 34-3: Example output for LW4o6 (config method DHCP)

```
awplus#show software-configuration

Software Configuration: lw4o6

Configuration Source: dhcp
Upstream Interface: eth1
MAP-E Version: rfc
lwAFTR Address: 2001:0db8:acc3:0055:0000:0000:0000:0001
lw4o6 Rule:
  IPv4-Address: 192.0.2.123
  IPv6-Prefix: 2001:0db8::/32
  PSID offset: 0
  PSID length: 9
  PSID: 346 (0x15a)

Border Relay Device: Not Set
```

**Related commands**

- [software-configuration](#)
- [method \(software\)](#)
- [br-address \(software\)](#)
- [upstream-interface](#)
- [rule \(software\)](#)

**Command changes** Version 5.4.9-0.1: command added

# software-configuration

**Overview** Use this command to enter the Software Configuration mode. This mode allows you to configure software settings.

In computer networking, a software is a type of tunneling protocol that creates a virtual "wire" that transparently encapsulates another protocol. Softwares are used for various purposes, one of which is to carry IPv4 traffic over IPv6 and vice versa, in order to support IPv6 transition mechanisms.

Use the **no** variant of this command to remove a software configuration.

**Syntax** `software-configuration <software-config-name>`  
`no software-configuration <software-config-name>`

| Parameter                                 | Description                                       |
|---|---|
| <code>&lt;software-config-name&gt;</code> | The name assigned for this software configuration |

**Mode** Global Configuration

**Example** To configure software settings for 'software1', use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration software1
awplus(config-software)#
```

To remove software 'software1', MAP Rules configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# no software-configuration software1
```

**Related commands** [show software-configuration](#)

**Command changes** Version 5.4.9-0.1: command added

# tunnel security-reprocessing

**Overview** Use this command to enable stream security reprocessing on all tunnel interfaces.

Use the **no** variant of this command to disable security reprocessing on all tunnel interfaces.

Note that tunnel security reprocessing increases the load on your device and reduces throughput. This is because traffic is processed twice through the DPI engine. Therefore, it should only be enabled if your solution requires it.

**Syntax** tunnel security-reprocessing  
no tunnel security-reprocessing

**Default** Security reprocessing is disabled by default.

**Mode** Global Configuration

**Usage notes** Use this command when you need to reinspect the traffic in a tunnel terminating on the device using stream UTM features after tunnel headers and encryption have been removed. For a configuration example using this command, see the [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#).

**Example** To enable security reprocessing, use the commands:

```
awplus# configure terminal  
awplus(config)# tunnel security-reprocessing
```

To disable security reprocessing, use the commands:

```
awplus# configure terminal  
awplus(config)# no tunnel security-reprocessing
```

**Related commands** [show interface tunnel \(IPsec\)](#)

**Command changes** Version 5.4.8-0.2: command added

# tunnel destination (DS-Lite)

**Overview** Use this command to specify the tunnel destination for a DS-Lite tunnel.  
Use the **no** variant of this command to remove a configured tunnel destination.

**Syntax** tunnel destination dhcp interface <interface-name>  
no tunnel destination

| Parameter        | Description                                  |
|------------------|--|
| <interface-name> | The interface which receives the DHCP reply. |

**Mode** Interface Configuration

**Example** To configure a DS-Lite tunnel destination, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel mode ds-lite
awplus(config-if)# tunnel destination dhcp interface eth1
```

To remove the tunnel destination, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# no tunnel mode destination
```

**Related commands** [tunnel mode ds-lite](#)

**Command changes** Version 5.4.9-0.1: command added



# tunnel mode ds-lite

**Overview** Use this command to set the tunnel mode to DS-Lite for a tunnel interface.  
Use the **no** variant of this command to remove the tunnel mode.

**Syntax** tunnel mode ds-lite  
no tunnel mode

**Default** Not set.

**Mode** Interface Configuration

**Example** To configure the DS-Lite tunnel mode on interface 'tunnel0', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel mode ds-lite
```

To remove the configured DS-Lite tunnel mode for 'tunnel0', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# no tunnel mode
```

**Related commands** [tunnel mode \(IPv6\)](#)

**Command changes** Version 5.4.9-0.1: command added

# tunnel mode lw4o6

**Overview** Use this command to set the tunnel mode to Light Weight 4over6 (lw4o6) for a tunnel interface.

Use the **no** variant of this command to remove an established lw4o6 tunnel.

**Syntax** tunnel mode lw4o6  
no tunnel mode

**Default** Not set.

**Mode** Interface Configuration

**Example** To configure lw4o6 tunnel mode for tunnel6, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel mode lw4o6
```

To removed the configured lw4o6 tunnel mode for tunnel6, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel mode
```

**Related commands** [tunnel mode \(IPv6\)](#)

**Command changes** Version 5.4.9-0.1: command added

# tunnel mode map-e

**Overview** Use this command to set the tunnel mode to MAP-E for a tunnel interface.  
Use the **no** variant of this command to remove the MAP-E mode from a tunnel interface.

**Syntax** tunnel mode map-e  
no tunnel mode

**Default** Not set.

**Mode** User Exec and Privileged Exec

**Example** To configure the MAP-E tunnel mode on interface 'tunnel6', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel mode map-e
```

To remove the configured MAP-E tunnel mode for 'tunnel6', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel mode
```

**Related commands** [show software-configuration](#)

**Command changes** Version 5.4.9-0.1: command added

# tunnel software

**Overview** Use this command to configure the software configuration to use for a tunnel interface.

Note that **tunnel-mode map-e** or **tunnel mode lw4o6** must be configured in order for the command **tunnel software** to be valid.

Use the **no** variant of this command to remove a tunnel software configuration.

**Syntax** tunnel software <software-config-name>  
no tunnel software

| Parameter              | Description  |
|------------------------|--|
| <software-config-name> | The software configuration used for a tunnel interface |

**Default** Not set.

**Mode** Interface Configuration

**Example** To set the software configuration called 'swconfig' to an interface called 'tunnel6', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel software swconfig
```

To remove the software configuration for interface 'tunnel6', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel software
```

**Related commands** tunnel mode map-e  
tunnel mode lw4o6

**Command changes** Version 5.4.9-0.1: command added

# upstream-interface

**Overview** Use this command to assign a software configuration to an upstream interface configured with a globally scoped IPv6 address.  
Use the **no** variant of this command to remove a configured upstream interface.

**Syntax** `upstream-interface <interface-name>`  
`no upstream-interface`

| Parameter                           | Description  |
|-------------------------------------|--|
| <code>&lt;interface-name&gt;</code> | Name of the interface connected to upstream (e.g. eth1, vlan1) |

**Default** Not set.

**Mode** SoftWire Configuration

**Example** To configure the software configuration ('swconfig') upstream-interface to eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# upstream-interface eth1
```

To remove the software configuration ('swconfig') upstream-interface configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# no upstream-interface
```

**Related commands** [show software-configuration](#)

**Command changes** Version 5.4.9-0.1: command added

# 35

# IPv6 Tunneling Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure IPv6 Tunneling.

For more information, see the [IPv6 Tunneling Feature Overview and Configuration Guide](#).

- Command List**
- ["interface tunnel \(IPv6\)"](#) on page 1383
  - ["ip address \(IP Addressing and Protocol\)"](#) on page 1384
  - ["ip tcp adjust-mss"](#) on page 1385
  - ["ipv6 address"](#) on page 1387
  - ["ipv6 tcp adjust-mss"](#) on page 1389
  - ["mtu"](#) on page 1391
  - ["show interface tunnel \(IPv6\)"](#) on page 1393
  - ["tunnel destination \(IPv6\)"](#) on page 1394
  - ["tunnel dscp"](#) on page 1396
  - ["tunnel mode \(IPv6\)"](#) on page 1397
  - ["tunnel source \(IPv6\)"](#) on page 1398
  - ["tunnel ttl"](#) on page 1400

# interface tunnel (IPv6)

**Overview** Use this command to create a tunnel interface or to enter Interface mode to configure an existing tunnel. Tunnel interfaces are identified by an index identifier that is an integer in the range from 0 through 65535.

Use the **no** variant of this command to remove a previously created tunnel interface.

**Syntax** `interface tunnel< tunnel-index >`  
`no interface tunnel< tunnel-index >`

| Parameter                           | Description  |
|-------------------------------------|--|
| <code>&lt; tunnel-index &gt;</code> | Specify a tunnel interface index identifier in the range from 0 through 65535. |

**Default** Tunnel interfaces do not exist.

**Mode** Global Configuration

**Usage notes** After you have created the tunnel interface, use the **tunnel mode** command to enable the tunnel.

**Examples** To configure a tunnel interface with index 30 and use IPv6 tunneling, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel30
awplus(config-if)# tunnel mode ipv6
```

To remove the IPv6 tunnel interface tunnel30, use the commands:

```
awplus# configure terminal
awplus(config)# no interface tunnel30
```

**Command changes** Version 5.4.8-2.1: command added

# ip address (IP Addressing and Protocol)

**Overview** This command sets a static IP address on an interface.  
The **no** variant of this command removes the IP address from the interface.

**Syntax** `ip address <ip-addr/prefix-length>`  
`no ip address [<ip-addr/prefix-length>]`

| Parameter                                  | Description  |
|--|--|
| <code>&lt;ip-addr/prefix-length&gt;</code> | The IPv4 address and prefix length you are assigning to the interface. |

**Mode** Interface Configuration for a VLAN interface, a local loopback interface, a PPP interface, or a tunnel.

**Examples** To add the IP address 10.10.10.50/24 to the interface `vlan1`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip address 10.10.10.50/24
```

To add the IP address 10.10.11.50/24 to the local loopback interface `lo`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.11.50/24
```

To add the IP address 10.10.11.50/24 to the PPP interface `ppp0`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip address 10.10.11.50/24
```

To add the IP address 10.10.11.50/24 to the tunnel `tunnel0`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# ip address 10.10.11.50/24
```

**Related commands** [interface \(to configure\)](#)  
[show ip interface](#)  
[show running-config interface](#)



# ip tcp adjust-mss

**Overview** Use this command to set the Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

**Syntax** `ip tcp adjust-mss {<mss-size>|pmtu}`  
`no ip tcp adjust-mss`

| Parameter                     | Description  |
|-------------------------------|--|
| <code>&lt;mss-size&gt;</code> | <code>&lt;64-1460&gt;</code> Specifies the MSS size in bytes.          |
| <code>pmtu</code>             | Adjust TCP MSS automatically with respect to the MTU on the interface. |

**Default** The default setting allows a TCP server or a TCP client to set the MSS value for itself.

**Mode** Interface Configuration

**Usage notes** When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel
- VLAN

**Examples** To configure an MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ip tcp adjust-mss 1452
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip tcp adjust-mss
```

**Related  
commands**

[mtu \(PPP\)](#)  
[show interface](#)  
[show interface \(PPP\)](#)

**Command  
changes**

Version 5.4.8-2.1: interface tunnel example added

# ipv6 address

**Overview** Use this command to set the IPv6 address of an interface. The command also enables IPv6 on the interface, which creates an EUI-64 link-local address as well as enabling RA processing and SLAAC.

To stop the device from processing prefix information (routes and addresses from the received Router Advertisements) use the command **no ipv6 nd accept-ra-pinfo**.

To remove the EUI-64 link-local address, use the command **no ipv6 eui64-linklocal**.

Use the **no** variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

**Syntax** `ipv6 address <ipv6-addr/prefix-length>`  
`no ipv6 address <ipv6-addr/prefix-length>`

| Parameter                                    | Description   |
|--|---|
| <code>&lt;ipv6-addr/prefix-length&gt;</code> | Specifies the IPv6 address to be set. The IPv6 address uses the format X:X::X/Prefix-Length. The prefix-length is usually set between 0 and 64. |

**Mode** Interface Configuration for a VLAN interface, a PPP interface, or a tunnel.

**Usage notes** 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 vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the VLAN interface vlan1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

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 assign the IPv6 address to the tunnel tunnel0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
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
```

**Related  
commands**

- [ipv6 address autoconfig](#)
- [ipv6 address dhcp](#)
- [ipv6 dhcp server](#)
- [ipv6 enable](#)
- [ipv6 eui64-linklocal](#)
- [show running-config](#)
- [show ipv6 interface brief](#)
- [show ipv6 route](#)

# ipv6 tcp adjust-mss

**Overview** Use this command to set the IPv6 Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

**Syntax** `ipv6 tcp adjust-mss {<mss-size>|pmtu}`  
`no ipv6 tcp adjust-mss`

| Parameter                     | Description  |
|-------------------------------|--|
| <code>&lt;mss-size&gt;</code> | <code>&lt;64-1460&gt;</code> Specifies the MSS size in bytes.          |
| <code>pmtu</code>             | Adjust TCP MSS automatically with respect to the MTU on the interface. |

**Default** The default setting allows a TCP server or a TCP client to set the MSS value for itself.

**Mode** Interface Configuration

**Usage notes** When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel
- VLAN

**Examples** To configure an IPv6 MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To configure an IPv6 MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To adjust IPv6 TCP MSS automatically with respect to the MTU on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ipv6 tcp adjust-mss pmtu
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 tcp adjust-mss
```

**Related  
commands**

[mtu \(PPP\)](#)  
[show interface](#)  
[show interface \(PPP\)](#)

**Command  
changes**

Version 5.4.8-2.1: interface tunnel example added

# mtu

**Overview** Use this command to set the Maximum Transmission Unit (MTU) size for interfaces, where MTU is the maximum packet size that interfaces can transmit. The MTU size setting is applied to both IPv4 and IPv6 packet transmission.

Use the **no** variant of this command to remove a previously specified Maximum Transmission Unit (MTU) size, and restore the default MTU size. For example the VLAN interface default is 1500 bytes.

**Syntax** `mtu <68-1582>`  
`no mtu`

**Default** The default MTU size, for example 1500 bytes for VLAN interfaces.

**Mode** Interface Configuration

**Usage notes** If a device receives an IPv4 packet for Layer 3 switching to another interface with an MTU size smaller than the packet size, and if the packet has the **'don't fragment'** bit set, then the device will send an ICMP **'destination unreachable'** (3) packet type and a **'fragmentation needed and DF set'** (4) code back to the source. For IPv6 packets bigger than the MTU size of the transmitting interface, an ICMP **'packet too big'** (ICMP type 2 code 0) message is sent to the source.

You can set a feasible MTU value on the following interfaces:

- PPP
- Ethernet
- Tunnel
- VLAN

Note that you cannot configure MTU on bridge interfaces. The MTU of the bridge interface is determined by the member interface of the bridge which has the lowest MTU. For example, if you attach eth1 with MTU 1200, ppp1 with MTU 1400, and vlan1 with MTU 1500 to a bridge interface, the MTU for that interface will be 1200.

Note that `show interface` output will only show MTU size for VLAN interfaces.

**Examples** To configure an MTU size of 1500 bytes on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# mtu 1500
```

To configure an MTU size of 1500 bytes for tunnel "tunnel2", use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# mtu 1500
```

To restore the MTU size to the default MTU size of 1500 bytes on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no mtu
```

**Related commands** [show interface](#)



# show interface tunnel (IPv6)

**Overview** Use this command to display status information of tunnels.

The tunnel remains inactive if no valid tunnel source or tunnel destination is configured.

**Syntax** `show interface tunnel<tunnel-index>`

| Parameter | Description  |
|-----------|--|
| tunnel    | Specify this parameter to display tunnel status information of a given tunnel identified by the <0-255> parameter. |
| <0-255>   | Specify a tunnel index in the range from 0 through 255.  |

**Mode** Privileged Exec

**Example** To display status information for IPv6 tunnel tunnel120, use the command:

```
awplus# show interface tunnel120
```

Figure 35-1: Example output from the **show interface tunnel** command

```
awplus#show interface tunnel120
Interface tunnel120
  Link is UP, administrative state is UP
  Hardware is Tunnel
  IPv4 address 192.168.10.1/24 pointopoint 192.168.10.255
  index 4751 metric 1 mtu 1480
  arp ageing timeout 300
  <UP,POINTOPOINT,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  Tunnel source 2001:db8::1:1, destination 2001:db8::2:1
  Tunnel name local 2001:db8::1:1, remote 2001:db8::2:1
  Tunnel ID local (not set), remote (not set)
  Tunnel protocol/transport ipv6, key disabled, sequencing disabled
  Tunnel TTL 64
  Checksumming of packets disabled, path MTU discovery disabled
  input packets 0, bytes 0, dropped 0, multicast packets 0
  output packets 0, bytes 0, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 22:38:35
```

**Command changes** Version 5.4.8-2.1: command added

# tunnel destination (IPv6)

**Overview** Use this command to specify a tunnel destination for the remote end of the tunnel. Tunnel destination can be specified by using a destination network name or an IPv6 address.

Use the **no** variant of this command to remove a configured tunnel destination.

**Syntax** tunnel destination {<ipv6-addr>|<destination-network-name>}  
no tunnel destination

| Parameter                  | Description  |
|----------------------------|--|
| <ipv6-addr>                | Specify the tunnel destination IPv6 address in the dotted decimal format x::x:x. The endpoints of the tunnel must be configured by mirroring IP addresses, that is, the tunnel source on one endpoint must be specified as the tunnel destination on the other endpoint. |
| <destination-network-name> | Destination network name. If the destination network name cannot be resolved, then the IPv6 tunnel remains inactive.   |

**Mode** Interface Configuration

**Examples** To configure an IPv6 tunnel destination by using an IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode ipv6
awplus(config-if)# tunnel destination 2001:db8::1:1
```

To configure an IPv6 tunnel destination by using a destination network name, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode ipv6
awplus(config-if)# tunnel destination
corporate_lan.example.com
```

To remove a IPv6 tunnel destination, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# no tunnel destination
```

**Related commands** [interface tunnel \(IPv6\)](#)  
[tunnel mode \(IPv6\)](#)

tunnel source (IPv6)

**Command changes** Version 5.4.8-2.1: command added

# tunnel dscp

**Overview** Use this command to configure the Differentiated Services Code Point (DSCP) value for the DSCP field in the packet header that encapsulates the tunneled packets.

Use the **no** variant of this command to reset the DSCP field to its default value.

**Syntax** tunnel dscp <0-63>  
no tunnel dscp

| Parameter | Description   |
|-----------|---|
| <0-63>    | Specify the DSCP value in the range from 0 through 63 for the DSCP field in the packet header that encapsulates the tunneled packets. |

**Default** The IPv4 DSCP field value is inherited from the inner header to the outer header.

**Mode** Interface Configuration

**Examples** To configure the DSCP value to 10 for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel dscp 10
```

To remove a configured DSCP value for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel dscp
```

**Related commands** [interface tunnel \(IPv6\)](#)

# tunnel mode (IPv6)

**Overview** Use this command to configure the encapsulation tunneling mode to use. This command sets IPv6 tunneling.

Use the **no** variant of this command to remove an established tunnel.

**Syntax** `tunnel mode ipv6`  
`no tunnel mode`

**Default** Virtual tunnel interfaces have no mode set by default.

**Mode** Interface Configuration

**Usage notes** A tunnel will not become operational until it is configured with this command.

**Examples** To configure IPv6 as the encapsulation mode for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode ipv6
```

To remove a configured IPv6 tunnel mode for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel mode
```

**Related commands** [interface tunnel \(IPv6\)](#)

**Command changes** Version 5.4.8-2.1: command added

# tunnel source (IPv6)

**Overview** Use this command to specify a tunnel source for the tunnel interface. Tunnel source can be specified by using an interface name or an IPv6 address. The source address must be an existing IPv6 address configured for an interface.

Use the **no** variant of this command to remove a tunnel source for a tunnel interface.

**Syntax** tunnel source {<ipv6-addr>|<interface-name>}  
no tunnel source

| Parameter        | Description   |
|------------------|---|
| <ipv6-addr>      | Specify the tunnel source IPv6 address for the IPv6 tunnel interface in the dotted decimal format x::x:x. The endpoints of the tunnel must be configured by mirroring IP addresses, that is, the tunnel source on one endpoint must be specified as the tunnel destination on the other endpoint. |
| <interface-name> | Available interface name. Any AlliedWare Plus interface type (eth, vlan, ppp, tunnel, lo and so on). Using interface name can minimize the number of user-configured IP addresses and allow the tunnel source IP address to be dynamically issued via, for example, DHCP.                         |

**Mode** Interface Configuration

**Examples** To configure an IPv6 tunnel source IPv6 address, use the commands:

```
awplus# configure terminal
awplus# interface eth1
awplus(config-if)# ip address 2001:db8::1:1/48
awplus(config-if)# interface tunnel1
awplus(config-if)# tunnel mode ipv6
awplus(config-if)# tunnel source 2001:db8::1:1
```

To use an interface name as the tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode ipv6
awplus(config-if)# tunnel source eth1
```

To remove an IPv6 tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel source
```

**Related commands** interface tunnel (IPv6)  
tunnel destination (IPv6)  
tunnel mode (IPv6)

**Command changes** Version 5.4.8-2.1: command added

# tunnel ttl

**Overview** Use this command to configure the value to use for the Time to Live (TTL) field in the IPv4 header that encapsulates the tunneled IPv4 or IPv6 packets.

Use the **no** variant of this command to set the TTL value to its default.

**Syntax** tunnel ttl <1-255>  
no tunnel ttl

| Parameter | Description                   |
|-----------|-------------------------------|
| <1-255>   | TTL value from 1 through 255. |

**Default** The default TTL value is inherited from the encapsulated packet.

**Mode** Interface Configuration

**Example** To set the TTL value of the packet to 255, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel20
awplus(config-if)# tunnel ttl 255
```

To remove the configured TTL value of the packet, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel20
awplus(config-if)# no tunnel ttl
```

**Related commands** [interface tunnel \(IPv6\)](#)